Na temelju članka 13. Statuta Fakulteta zdravstvenih studija Sveučilišta u Rijeci (Klasa: 003-05/18-02/08 PT od 06. travnja 2018.), dekan Fakulteta donosi sljedeći

PRAVILNIK O SIGURNOSTI INFORMACIJSKIH SUSTAVA

UVODNE ODREDBE

Članak 1.

Ovim se Pravilnikom uređuje sigurnost upravljanja informacijskim sustavima na Fakultetu zdravstvenih studija u Rijeci (dalje: Fakultet), definiraju prihvatljivi načini ponašanja i jasna raspodjela uloga i odgovornosti svih čimbenika informacijskog sustava.
Novi su se zaposlenici dužni upoznati s njegovim odredbama prilikom zapošljavanja, a studenti i gosti 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,
- informatički tim informacijskih sustava na Fakultetu,
- korisnike, među koje spadaju: zaposlenici, vanjski suradnici, studenti i gosti
- vanjske tvrtke koje po ugovoru rade na održavanju mrežne opreme ili softvera.

ORGANIZACIJA UPRAVLJANJA SIGURNOŠĆU

Članak 2.

Osobe koje se u radu koriste računalima dijele se na poružatelje i korisnike informatičkih usluga.

Pružateljima informatičkih usluga smatraju se profesionalci koji brinu o radu računala, mreže i informacijskih sustava.
Korisnici informatičkih usluga su osobe koje se u svom radu ili učenju služe računalima, izrađuju dokumente ili unose podatke, ali ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i mreže.

Korisnici informatičkih usluga obvezuju se:

- pridržavati se pravila prihvatljivog korištenja, odnosno ne koristiti računala za radnje koje nisu u skladu s važećim zakonima, etičkim i moralnim normama, Etičkim kodeksom Sveučilišta u Rijeci i sigurnosnom politikom Fakulteta,
- koristiti službenu elektroničku poštu Fakulteta kao službeno sredstvo komunikacije,
- u slučaju dobivanja sumnjive elektroničke pošte postupiti s razumnim oprezom (ne slijediti poveznice i otvarati priloge) ukoliko je riječ o sumnjivom pošiljatelju. O svim takvim porukama potrebno je u što kraćem vremenu obavijestiti informatičara,
- izabrati dovoljno jaku zaporku (veliko, malo slovo, broj, specijalan znak) i povremeno je mijenjati,
- prijaviti svaki sigurnosni incident, oštećenje ili kvar na računalu informatičaru Fakulteta

Korisnicima je zabranjeno:

- isključivanje i ometanje rada sustava za nadzor, upravljanje i zaštitu računala,

- namjerno unošenje zločudnih programa u mrežne sustave i servere (virusi, crvi, trojanjski konj),
- odavanje zaporke drugim osobama ili dopuštanje uporabe vlastitog korisničkog računa (user account) drugim osobama, neovisno o tome jesu li te osobe djeatnici Fakulteta,
- neovlašteno mijenjanje/dodavanje hardverske konfiguracije sustava ili dijela sustava (računala) korištenje neovlaštenih programa koji ne zahtjevaju instalaciju („portabilnu aplikacija"),
- lažno predstavljanje ili davanje korisničkog imena i zaporke drugoj osobi čime se omogućuje lažno predstavljanje.

Članak 3.

Dokumenti u elektroničkom obliku smatraju se službenim dokumentima na isti način kao i dokumenti na papiru, pa treba osigurati njihovo čuvanje i pristup samo ovlaštenim osobama.

Članak 4.

Svaka aplikacija koju Fakultet koristi za obradu podataka, a koja je od vitalne važnosti za Fakultet ili njegov dio, mora imati administratora/informatičara.
Administratora aplikacije određuje dekan na temelju specifičnosti pojedine aplikacije i odgovornosti zaposlenika.
Administrator je odgovaran za provjeru ispravnosti podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podacima i za mjere sprečavanja izmjene podataka od strane neautoriziranih osoba.
Administrator kontaktira proizvođača aplikacije i dogovara isporuku novih verzija, traži ugradnju sigurnosnih mehanizama, itd. ukoliko nije drugačije određeno.

Članak 5.

Osobe čija je zadaća sigurnost informacijskih sustava na Fakultetu čini informatički tim koji se sastoji od: administratora, informatičara Fakulteta i informatičkih referenata (vanjski suradnici).
Zajednička briga tima je ukupna sigurnost informacijskih sustava, što uključuje i fizičku sigurnost, pri čemu surađuju sa svim zaposlenicima i studentima na Fakultetu, nadziru rad mreže i ostalih servisa, sudjeluju hitnim u intervencijama i slično.
Informatički tim, također u dogovoru s Upravom sudjeluje u donošenju odluka o nabavi računala i softvera koji su neophodni za neometani rad sustava.

Članak 6.

Pružatelji usluga obvezni su administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.
Svako računalo ima imenovanog informatičkog referenta, koji odgovara za instalaciju i konfiguraciju softvera, a administrator evidentira zaduženja informatičkih referenata po računalima.
Računala se moraju konfigurirati na taj način da budu zaštićena od napada izvana i iznutra, što se osigurava instaliranjem softverskih zakrpi po preporukama proizvođača, listama pristupa, filtriranjem prometa i drugim sredstvima.
Posebnu pažnju informatičer i informatički referenti su obvezni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa (npr. Server).
Pružatelji informatičkih usluga ne smiju administrirati računala i mrežnu opremu koja je u vlasništvu privatnih i poslovnih korisnika.

Članak 7.

Informatičar i informatički referenti računala svakodnevno prate rad sustava, čitaju dnevničke zapise i provjeravaju rad servisa, nadgledaju rad korisnika, kako bi se otkrile nedopuštene aktivnosti.

Također su u obvezi prijaviti incidente 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. Ukoliko je incident ozbiljan i uključuje kršenje zakona, prijavljuju se CARNetovu CERT-u.
Pružatelji usluga obvezni 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 8.

Upravljanje mrežom, konfiguriranje mrežnih uređaja, dodjeljivanje mrežnih adresa, kreiranje virtualnih LAN-ova, te ostale poslove pri upravljanju mrežom vrše informatičer i informatički referenti.
Informatičar i informatički referenti obvezni su voditi Popis mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala.
Administratori CARNet-ovih poslužitelja dužni su voditi Popis javnih adresa računala.

Članak 9.

Računala koja posjednuju gostujući suradnici (vanjski suradnici, predavači, poslovni partneri i serviseri) smiju se priključiti na lokalnu mrežu samo uz prethodnu najavu uz pristutnost informatičara i na za to predviđenim mjestima (informatička učionica i predavaonice).
Korištenje bežičnih mrežnih resursa omogućiti će se svim pojedincima koji posjeduju AAI@EduHr elektronički identitet putem globalne roaming usluge Eduroam ili na drugim izoliranim pristupnim točkama uz odgovarajuće metode enkripcije i autentifikacije uređaja i korisnika, te ostale sigurnosno važne postavke.

Članak 10.

Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva.
Dekan zadužuje odgovornu osobu za instaliranje softvera i njegovo licenciranje (administrator).
Korisnik koji ima potrebu za nekim programom, mora se obratiti ovlaštenoj osobi i zatražiti, uz obrazloženje, nabavu i instalaciju.
Administrator za programsku podršku na Fakultetu poduzima daljnje radnje za nabavku uz suradnju Službe za nabavu.

SIGURNOST INFORMATIČKE OPREME

Članak 11.

Prostor u ustanovi dijeli se na dio koji je otvoren za javnost (studentski prostori, predavaonice), prostor u kojem imaju pristup samo zaposleni (uredi, kabineti, server sobe i sl.), te prostore u koje pristup imaju samo grupe zaposlenih (kabineti, dvorane, informatička učionica), ovisno o vrsti posla koji obavljaju.

Članak 12.

Oprema koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskog sustava ili sadrži povjerljive informacije, fizički se odvaja u prostor u koji je ulaz dozvoljen samo ovlaštenim osobama.
Administrator informatičkog tima obvezan je održavati popis ovlaštenih osoba koje imaju pristup u sigurne zone. U pravilu je to informatičar ili informatički referenti koji administriraju mrežnu i komunikacijsku opremu i poslužitelje ključnih servisa. Oni ulaze u sigurne zone samo kada treba ukloniti zastoje, obaviti servisiranje opreme.
Kritična 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 oporavak. U sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

Članak 13.

U navedene prostorije pristup nije dozvoljen osobama koje nisu korisnici usluga ni studentima, a dozvoljen je samo onim osobama koje je za to ovlastilo dekan Fakulteta.

Članak 14.

Povremeno se mora dopustiti pristup trećim osobama iz vanjskih tvrtki ili ustanova, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija, itd.

Fakultet može u ugovore s vanjskim tvrtkama odrediti odredbe kojima obavezuje poslovne partnere na poštivanje sigurnosnih pravila.

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.

Fakultet može zahtijevati da svaka osoba koja pristupa povjerljivoj opremi, sigurnoj zoni ili osjetljivim informacijama potpiše Izjavu o čuvanju povjerljivih informacija.

U slučaju da u sigurnu zonu radi potrebe posla ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja. Ukoliko se vanjskoj tvrtki prepušta održavanje opreme i aplikacija s povjerljivim podacima, Fakultet 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 Fakultet.

Fakultet zadržava pravo da osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup ukoliko nisu na popisu ovlaštenih djelatnika.

Članak 15.

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

- intranet - privatna mreža Fakulteta, koju čine poslužitelji internih servisa, osobna računala zaposlenih, informatička učionica te komunikacijska oprema lokalne mreže,
- extranet - proširenje privatne mreže na mobilne korisnike, poslovne partnere ili na izdvojene lokacije; u ovu grupu spadaju interni modemski ulazi (ako ih Fakultet ima), veze lokalnih baza podataka sa središnjim poslužiteljima (LDAP, ISVU, X-ice,) i sl.

Članak 16.

Fakultet je obavezan održavati popis sve računalne opreme, s opisom ugrađenih komponenti, inventarskim brojevima itd.

Fakultet je obvezan osoblju CARNeta dozvoliti pristup opremi u vlasništvu CARNeta koja se nalazi na Fakultetu.

Za fizičku sigurnost opreme odgovoran je dekan. On odgovornost za grupe uređaja ili pojedine uređaje prenosi na druge zaposlene, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.

Računalna oprema koja pripada Fakultetu daje se korisnicima na raspolaganje radi obavljanja poslova vezanih uz redovno poslovanje Fakulteta i nije ju dopušteno koristiti za obavljanje privatnih poslova korisnika.

Fakultet zadržava pravo nadzora nad načinom korištenja računalne opreme.

Korisnici koji opremu koriste izvan prostora Fakulteta odgovorni su za tu opremu kao i za sve posljedice koje proizlaze iz korištenja iste.

OSIGURANJE NEPREKIDNOSTI POSLOVANJA

Članak 17.

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 se stavak prvenstveno odnosi na kopije sustava središnjih poslužitelja, računovodstvenih podataka, podataka o audio-video zapisu i podataka o konfiguraciji softvera neophodnog za funkcioniranje mreže.

Članak 18.

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, nadležn je informatički tim..

Članak 19.

Fakultet je svim djelatnicima administrativnih službi osigurao uređaje za pohranu poslovnih podataka (USB), čime se podrazumijeva da svaki korisnik redovito vrši pohranu (*„back up"*) podataka s računala.

Informatičar je zadužen za povremenu provjeru izrade rezervnih kopija i upotrebljivost rezervnih kopija podataka.

Korisnici su obvezni uređaje za pohranu podataka čuvati na sigurnom mjestu i ne davati ga trećim osobama.

KORIŠTENJE RAČUNALNE OPREME FAKULTETA

Članak 20.

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 Fakultet.

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.),
- 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 Fakultetu,
- korištenje računala Fakulteta i ostalih informatičkih resursa Fakulteta u svrhe koje nisu u skladu s Etičkim kodeksom Sveučilišta u Rijeci.

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 Fakultetu ili ne,
- napad uskraćivanjem resursa na druga računala,
- vrijeđanje i ponižavanje ljudi u internetskoj komunikaciji po vjerskoj, rasnoj, nacionalnoj ili nekoj drugoj pripadnosti,
- korištenje mrežnih resursa Fakulteta na način priključivanja vlastitih – privatnih računala na računalnu mrežu Fakulteta.

Članak 21.

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

NADZOR NAD INFORMACIJSKIM SUSTAVIMA

Članak 22.

Fakultet zadržava pravo nadzora nad instaliranim softverom i podacima koji su pohranjeni na umreženim 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 informatičkog tima.
Pri provođenju nadzora ovlaštene su osobe dužne 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 23.

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 Fakulteta, ili oprema Fakulteta služi za njezin prijenos,
- pristup radnom prostoru (uredu, kabinetu, predavaonici, sigurnoj zoni, itd.),
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Fakulteta.

Članak 24.

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

Članak 25.

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

- poslužiteljima elektroničke pošte - ovlašteni CARNet sistem inženjeri,
- na internim poslužiteljima Fakulteta - djelatnici informatičkog timaili CARNet sistem inženjeri,
- svakom osobnom računalu korisnika – djelatnici informatičkog tima

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

Članak 26.

Osobe koje provode antivirusnu zaštitu dužne su instalirati antivirusne programe na sva korisnička računala i podesiti ih na način da se izmjene u bazi virusa automatski propagiraju s središnje instalacije ili s vanjskog poslužitelja, bez aktivnog sudjelovanja korisnika.

Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti antivirusni program, moraju zatražiti dozvolu od nadležnih pružatelja informatičkih usluga.

Članak 27.

Djelatnici informatičkog tima obvezan je postaviti poslužitelje elektroničke pošte tako da se prilikom primanja poruka konzultiraju 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.

Članak 28.

Svi zaposlenici Fakulteta, suradnici i studenti koji u svome radu koriste računala obvezni su pridržavati se u nastavku navedenih pravila korištenja zaporki, dok su ih djelatnici informatičkog tima obvezni tehnički ugraditi u sve sustave koji to omogućavaju.

Minimalna dužina zaporke mora biti šest znakova. Za zaporku se ne smiju koristiti riječi iz rječnika, niti imena bliskih osoba, ljubimaca, datuma i sl. U zaporci treba izmiješati mala i velika slova s brojevima i specijalnim znakovima.

Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni djelatnicima informatičkog tima. Korisnik je odgovoran za tajnost svoje zaporke, te mora naći način da je sakrije.

Članak 29.

Na računalima koja spadaju u zonu visokog rizika djelatnici informatičkog tima su obvezni konfigurirati sustav na taj način da se korisnički račun zaključa nakon tri neuspjela pokušaja prijave.

Djelatnici informatičkog tima su obvezni konfigurirati autentifikaciju tako da zaporke zastare nakon 90 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 Fakultet može stegovno djelovati ili postaviti zaposlenika na radno mjesto na kojem je manja mogućnost ugrožavanja integriteta i sigurnosti sustava i podataka.

RJEŠAVANJE SIGURNOSNIH INCIDENATA

Članak 30.

Svaki zaposlenik, student ili suradnik Fakulteta dužan je prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd. Informatičar Fakulteta treba izraditi, dokumentirati i održavati kontakt listu osoba kojima se prijavljuju problemi u radu mreže, mrežnih servisa i mrežne opreme.

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.

Djelatnici informatičkog tima smiju pratiti korisničke procese. Ukoliko postoji opravdana sumnja da se računalo koristi na nedozvoljen način, može se provjeriti sadržaj korisničkog direktorija, ali se ne smiju provjeravati sadržaji korisničkih podatkovnih datoteka (npr. dokumenata ili e-mail poruka).
Daljnju istraga može se provesti samo ako je prijavljena administratoru uz poštivanje slijedećih pravila:

- istragu provodi jedna osoba, ali uz prisustvo svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama,
- informacijski se sustav mora sačuvati u zatečenom stanju, odnosno ne smiju se učiniti izmjene koje bi otežale ili onemogućile dijagnosticiranje,
- stvara se kopija zatečenog stanja (npr. na, cd, usb, ...), po mogućnosti na takav način da se ne izmijene atributi datoteka (na Unixu naredbom dd),
- dokumentira se svaka radnja, tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage,
- istražnom se postupku piše izvještaj, kako bi u slučaju potrebe mogao poslužiti kao dokaz u stegovnim ili sudskim procesima,
- izvještaji o incidentu smatraju se povjerljivim dokumentima i čuvaju se na taj način da im pristup imaju samo ovlaštene osobe.

Fakultet može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija. Detaljnu istragu nakon prijave vrši CARNetov CERT.

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.
Fakultet može osobama odgovornim za sigurnosni incident zabraniti fizički pristup prostorijama ili logički pristup podacima.
Ukoliko je incident izazvao zaposlenik vanjske tvrtke, Fakultet može zatražiti od vanjske tvrtke da ga ukloni s liste osoba ovlaštenih za obavljanje posla na ustanovi. U slučaju teže povrede pravila sigurnosne politike, Fakultet može raskinuti ugovor s vanjskom tvrtkom.

ZAVRŠNE ODREDBE

Članak 34.

Ovaj Pravilnik o sigurnosti informacijskog sustava stupa na snagu danom objave na oglasnoj ploči i mrežnim stranicama Fakulteta.

DEKAN

SVEUČILIŠTE U RIJECI
FAKULTET ZDRAVSTVENIH STUDIJA
RIJEKA

Prof. dr. sc. Alan Šustić, dr. med.

Klasa: 003-05/18-02/36
Ur. broj: 2170-57-5-01-18-1
Rijeka, 02. listopada 2018.

Objavljeno na oglasnoj ploči i mrežnim stranicama Fakulteta dana 03. listopada 2018.

TAJNICA FAKULTETA

SVEUČILIŠTE U RIJECI
FAKULTET ZDRAVSTVENIH STUDIJA
RIJEKA

Iva Križanec Ropac, dipl. iur.