Na temelju članka 34. Statuta Veterinarskoga fakulteta Sveučilišta u Zagrebu, a u svezi s Nacionalnim programom informacijske sigurnosti u Republici Hrvatskoj, Fakultetsko vijeće u širem sastavu na sjednici održanoj dana 22. studenoga 2006. godine donijelo je

P R A V I L N I K

o sigurnosnoj politici i sigurnosti informacijskoga sustava Veterinarskoga fakulteta Sveučilišta u Zagrebu

Članak 1.

Pravila rada i ponašanja koja definira sigurnosna politika vrijede za:

- **korisnike** (zaposlenici, vanjski suradnici i studenti);
- **davatelje informacijskih usluga** (specijalisti za sigurnost, administratori informacijskih sustava);
- **vanjske tvrtke** koje po ugovoru rade na održavanju opreme ili softvera;
- **računalnu i programsku opremu** koja se nalazi u prostorima Veterinarskoga fakulteta (u daljnjem tekstu Fakulteta).

Članak 2.

Korisnici informatičkih usluga su

- osobe koje se u svom radu ili učenju služe računalima, proizvode dokumente ili unose podatke, ali ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i mreže. Korisnik informacijskog sustava mora znati koja je njegova uloga u poboljšanju sigurnosti ukupnog sustava.

Članak 3.

Dužnosti korisnika:

- pridržavanje pravila prihvatljivog korištenja, što znači da ne smiju koristiti računala za djelatnosti koje nisu u skladu s važećim zakonima, etičkim normama i pravilima lokalne sigurnosne politike;
- izbor kvalitetne zaporke i njezina povremena promjena;
- prijavljivanje sigurnosnih incidenata kako bi se što prije riješili problemi;
- korisnici koji proizvode podatke i dokumente odgovorni su za njihovo čuvanje. Od davatelja usluga potrebno je zatražiti da uspostave automatsku pohranu (backup) važnih informacija, ili u protivnom moraju sami izrađivati sigurnosne kopije;

- korisnik ima pravo i obvezu na osobnom računalu obnavljati operativni sustav u skladu s dinamikom koju predlaže proizvođač operativnog sustava. U slučaju da korisnik nema stručno znanje, obvezu preuzima administrator na zahtjev korisnika;
- korisnik ima pravo i obvezu da na osobnom računalu koristi i obnavlja programe za zaštitu računala od neželjenih (malicioznih) programa (virusi i crvi, trojanski konji, dialeri, programi koji sakupljaju osobne podatke i šalju ih promidžbenim agencijama – spyware i adware). U slučaju da korisnik nema stručno znanje, obvezu preuzima administrator na zahtjev korisnika;
- dokumenti i podatci u elektroničkom obliku smatraju se službenim dokumentima na isti način kao i dokumenti na papiru, pa treba osigurati njihovo čuvanje i ograničiti pristup samo ovlaštenim osobama.

Članak 4.

Glavni korisnik

- Kod korištenja aplikacija za obradu podataka, (na primjer računovodstven program) radi poboljšanja sigurnosti, jedna se osoba imenuje glavnim korisnikom (primjer: voditelj računovodstva bio bi glavni korisnik).
- Glavni je korisnik odgovaran za provjeru ispravnosti podataka, za provjeru ispravnosti i sigurnosti aplikacije, za dodjelu dozvola za pristup podatcima i za mjere sprečavanja izmjene podataka od strane neautoriziranih osoba.
- Glavni korisnik kontaktira proizvođača aplikacije i dogovara isporuku novih verzija, traži ugradnju sigurnosnih mehanizama itd.

Članak 5.

Davatelji informatičkih usluga

- Davateljima usluga smatraju se profesionalci koji brinu o radu računala, mreže i informacijskih sustava. Na ustanovama članicama CARNeta to su sistem inženjer i članovi njegova tima. Oni odgovaraju za ispravnost i neprekidnost rada informacijskog sustava.

Članak 6.

Specijalisti za sigurnost

- Veterinarski fakultet može za brigu o sigurnosti i pomoć pri rješavanju incidenata koristiti pomoć CARNeta. Usprkos tome, preporučuje se imenovanje i obrazovanje pojedinaca čija je zadaća briga za organizaciju i provođenje sigurnosnih mjera navedenih u Sigurnosnoj politici.
- Osoba čije je prvenstvena briga sigurnost informacijskih sustava je voditelj sigurnosti. Poželjno je da voditelj sigurnosti bude stručan, ali da istovremeno posjeduje sposobnost za

vođenje ljudi i da je komunikativan. Njegova je briga ukupna sigurnost informacijskih sustava. To uključuje fizičku sigurnost, pri čemu će surađivati sa zaposlenicima poput portira, čuvara i slično. Voditelj sigurnosti piše pravilnike, nadzire rad mreže i servisa, organizira obrazovanje korisnika i administratora, komunicira s upravom, sudjeluje u donošenju odluka o nabavi računala i softvera, te sudjeluje u razvoju softvera, kako bi osigurao da se poštuju pravila iz sigurnosne politike.

- Ako Fakultet zapošljava više stručnjaka za računarstvo, potrebno je imenovati ekipu za hitne intervencije i obučiti je za postupanje u slučaju incidentnih situacija. Ekipu čine specijalisti različitih usmjerenja, na primjer za mrežu, Unix, Microsoft Windowse, baze podataka itd. Fakultet treba u tom slučaju razraditi procedure za postupanje u incidentnim situacijama, te obučiti članove Ekipe za hitne intervencije kako bi mogli obaviti istragu, te informacijski sustav što prije vratiti u redovito stanje.
- Procedura za rješavanje incidenata dana je u pratećem dokumentu pod nazivom "Pravilnik o rješavanju sigurnosnih incidenata".
- Fakultet treba izraditi i održavati kontakt listu s imenima, brojevima telefona, e-mail adresama osoba kojima se prijavljuju incidenti, od kvarova opreme, sporosti ili nedostupnosti mrežnih usluga i podataka, do povreda pravila sigurnosne politike ili zakonskih odredbi.

Članak 7.

Administratori i administriranje računala

- Svako računalo mora imati imenovanog administratora, koji odgovara za instalaciju i konfiguraciju softvera. Ukoliko napredni korisnici žele sami administrirati svoje osobno računalo neka potpišu izjavu o tome nakon čega za njih vrijede sva pravila za administriranje računala.
- Računala moraju biti jednoznačno imenovana kako bi administrator znao gdje je računalo smješteno. Preporuča se da u imenu računala bude sufiks od tri znaka koji označavaju radnu jedinicu, znak – (crtica bez razmaka ispred i iza) te naziv računala koji sadrži ime korisnika bez naših dijakritičkih znakova ili odjel (primjer: Int-iharapin; Int-laboratorij).
- 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.
- Administratori su dužni posvetiti posebnu pažnju opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa.
- 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 specijalistu za sigurnost, 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.
- Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla. Da bi ih Fakultet obvezao na poštivanje tih pravila, neka potpišu Izjavu o čuvanju povjerljivih informacija, čiji je predložak dan među pratećim dokumentima.

Članak 8.

Upravljanje mrežom

- Djelatnik zadužen za upravljanjem mrežom mora u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala, upravlja mrežom, konfigurira mrežne uređaje, dodjeljuje adrese, kreira virtualne LAN-ove, propisuje procedure za priključivanje računala u mrežu, određuje oblik obrasca kojima se izdaje odobrenje za priključenje računala na mrežu i dodjeljuje im se adresa.
- Ukoliko je podržan rad na daljinu, mora se osigurati da udaljeno računalo ne ugrozi sigurnost mreže Fakulteta, s obzirom na mogućnost da ga koriste neautorizirane osobe, članovi obitelji i slično. Povjerljivi podatci na udaljenom računalu moraju biti jednako sigurni kao da se računalo nalazi u zgradi Fakulteta.
- Djelatnik zadužen za upravljanjem mrežom obavezan je razraditi pravila za spajanje na mrežu gostujućih računala, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri, serviseri. Ne smije se dozvoliti da samovoljno priključuju računala na mrežu Fakulteta, radi opasnosti od širenja virusa ili namjernih agresivnih radnji, poput presretanja mrežnog prometa, prikupljanja informacija itd. Fakultet može odrediti priključna mjesta, na primjer u predavaonicama, gdje je dozvoljeno priključiti gostujuća računala, te konfiguracijom mreže spriječiti da se s tog segmenta mreže dopre do ostalih računala na ustanovi.
- Djelatnik zadužen za upravljanjem mrežom kod stvaranja bežične mreže mora osigurati da se ne može bilo tko priključiti na privatnu mrežu i snimati promet. To se postiže metodama enkripcije i autentikacije uređaja i korisnika, koji se moraju propisati u zasebnom dokumentu.
- Radi zaštite povjerljivih informacije pri prijenosu mrežom, poželjno je da takav promet bude kriptiran. Fakultet će u tom slučaju izdati pravilnik u kojem definira vrstu enkripcije, obvezan softver, procedure za dodjelu i čuvanje kriptografskih ključeva i slično.

Članak 9.

Povjerenstvo za sigurnost informacijskih sustava

- Povjerenstvo za sigurnost je sastavljeno od predstavnika uprave i specijalista tehničara (na primjer voditelj sigurnosti, CARNet koordinator, prodekan, glavni korisnik baze podataka koja sadrži povjerljive informacije itd.).
- Povjerenstvo prima izvještaje o sigurnosnoj situaciji i predlaže mjere za njezino poboljšanje, uključujući nabavu opreme, organizaciju obrazovanja korisnika i specijalista. Povjerenstvo daje odobrenje za provođenje istrage u slučaju incidenata.
- Povjerenstvo podnosi izvještaj o stanju sigurnosti upravi Fakulteta te se zalaže za donošenje konkretnih mjera, nabavu potrebne opreme, ulaganje u obrazovanje specijalista, ali i običnih korisnika.

Članak 10.

Vanjske tvrtke

- Povremeno se mora dopustiti pristup osobama iz vanjskih tvrtki ili ustanova, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja, konzultacija itd.
- Fakultet može u ugovore s vanjskim tvrtkama ugraditi odredbe kojima obvezuje 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 obvezati 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.
- 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 podatcima, ustanova može od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije Fakulteta 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.

Sigurnost opreme

Klasifikacija računalne opreme

Članak 11.

Podjela opreme prema zadaćama koje obavlja:

- **zona javnih servisa** (tzv. demilitarizirana zona) - oprema koja obavlja javne servise (DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte itd.);
- **intranet** je privatna mreža Veterinarskog fakulteta. Čine 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, na primjer interni modemski ulazi ili veza lokalnih baza podataka s centralnim poslužiteljima (LDAP, ISVU, X-ice).
  Potrebno je izraditi **poseban pravilnik za extranet** u kojem se reguliraju prava i obveze, a vanjske tvrtke kojima se dopušta pristup računalima i podatcima u intranetu treba ugovorom obvezati na poštivanje sigurnosnih pravila i čuvanje povjerljivosti informacija.

Članak 12.

Podjela opreme prema vlasništvu

- U prostorijama Fakulteta nalazi se i oprema CARNeta ili Ministarstva znanosti, obrazovanja i športa, koja je dana na korištenje Fakultetu.
- Fakultet je obvezan održavati popis sve računalne opreme, s opisom ugrađenih komponenti, inventarskim brojevima itd.
- Fakultet brine jednako o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik.
- Fakultet je dužan osoblju CARNeta dozvoliti pristup opremi u vlasništvu CARNeta koja se nalazi na Fakultetu.

Članak 13.

Odgovornost za računalnu opremu

- Za fizičku sigurnost opreme odgovoran je rukovoditelj Fakulteta. On odgovornost za grupe uređaja ili pojedine uređaje prenosi na druge zaposlene, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.
- Fakultet je dužan razraditi procedure kojima se nastoji spriječiti otuđenje i oštećenje računalne opreme. Treba provjeriti ima li oprema koja se iznosi potrebne prateće dokumente, izdatnice, radne naloge za popravak itd.

Članak 14.

Fizička sigurnost

- Prostor na Fakultetu 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.
- Fakultet je dužan sastaviti popis osoba koje imaju pristup u zaštićena područja, a porta mora imati popis osoba koje mogu dobiti ključeve određenih prostorija.

Članak 15.

Sigurne zone

- Računalna 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.
- Fakultet je dužan 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.
- Kritična oprema treba biti zaštićena od problema s napajanjem električnom energijom, što znači da električne instalacije moraju biti izvedene kvalitetno, da se koriste uređaji za neprekidno napajanje, a po potrebi i generatori električne energije.
- U sigurnim zonama i u njihovoj blizini ne smiju se držati zapaljive i eksplozivne tvari.

Članak 16.

Instalacija i licenciranje programske podrške (software)

- Fakultet zadužuje jednu ili više odgovornih osoba za instaliranje softvera i njegovo licenciranje. Korisnik koji treba neki program, mora se obratiti ovlaštenoj osobi i zatražiti, uz obrazloženje, nabavu i instalaciju.
- Sve korisnike treba obvezati na poštivanje autorskih prava čitanjem i potpisivanjem izjave o tome da su upoznati s Politikom prihvatljivog korištenja i da je prihvaćaju. Na taj način Fakultet odgovornost za eventualno kršenje zakona prebacuje na nesavjesnog korisnika.

Članak 17.

Osiguranje neprekidnosti poslovanja

- Potrebno je redovito izrađivati rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju softvera. Preporučuje se izrada više kopija, koje se čuvaju na različitim mjestima, po mogućnosti u vatrootpornim ormarima (u slučaju nezgoda poput kvarova na sklopovlju, požara, ili ljudskih grešaka).
- Procedure za izradu rezervnih kopija treba razraditi u zasebnom dokumentu. Potrebno je zadužiti konkretne djelatnike za izradu i čuvanje kopija informacija, te ih obvezati na čuvanje povjerljivosti informacija.
- Radi osiguranja neprekinutosti poslovanja, potrebno je razraditi i procedure za oporavak kritičnih sustava te ih čuvati u pisanom obliku, kako bi u slučaju zamjene izvršitelja novozaposleni djelatnici mogli brzo reagirati u slučaju nesreće.
- Povremeno se provjerava upotrebljivost rezervnih kopija podataka, te izvode vježbe oporavka sustava. Vježbe se ne izvode na produkcijskim računalima, već na rezervnoj opremi, u laboratorijskim uvjetima.

Članak 18.

Nadzor nad informacijskim sustavima

- Fakultet zadržava pravo nadzora nad instaliranim softverom i podatcima koji su pohranjeni na umreženim računalima, te nad načinom korištenja računala.
- Nadzor smiju obavljati samo osobe koje je Fakultet za to ovlastio.

- Nadzor se smije provoditi radi osiguranja integriteta, povjerljivosti i dostupnosti informacija i resursa, provođenja istrage u slučaju sumnje da se dogodio sigurnosni incident te provjere jesu li informacijski sustavi i njihovo korištenje usklađeni sa zahtjevima sigurnosne politike.
- Pri provođenju nadzora, ovlaštene osobe dužne su poštivati privatnost i osobnost korisnika i njihovih podataka. 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.
- Ova se pravila odnose na svu računalnu opremu koja se nalazi u prostorijama Fakulteta i priključena je u mrežu CARNet, na sav instalirani softver te na sve mrežne servise. Pravila su dužni poštivati i provoditi svi zaposleni, studenti i vanjski suradnici koji po ugovoru obavljaju određene poslove.

Članak 19.

Provođenje

- 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.
- Administratori računala i pojedinih servisa su dužni specijalistima za sigurnost pomagati pri istrazi.

Članak 20.

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, laboratoriju, sigurnoj zoni itd.);
- pravo na interaktivno nadgledanje i bilježenje prometa na mreži Fakulteta.

Nepridržavanje zaposlenika može se disciplinski kazniti ili mu uskratiti prava korištenja mreže i njezinih servisa.

Članak 21.

Prateći dokumenti:

- Pravilnik o rukovanju korisničkim imenima i zaporkama
- Pravilnik o korištenju elektroničke pošte
- Pravilnik o antivirusnoj zaštiti
- Pravilnik o zaštiti od spama
- Pravilnik o rješavanju sigurnosnih incidenata

- Pravilnik o upravljanju povjerljivim informacijama

Članak 22.

Pravilnik o rukovanju korisničkim imenima i zaporkama

- Korisničko ime i zaporka služe u svrhu autentikacije i identifikacije korisnika.
- Svi korisnici računala pri prijavi na računalo koje ima pristup mreži obvezni su koristiti korisničko ime i zaporku.
- Iznimno se na javnim računalima mogu koristiti javna korisnička imena i zaporke. Takva računala moraju imati ograničen pristup mreži, što određuje administrator.
- Pravila korištenja korisničkim imenima i zaporkama dužni su pridržavati se svi zaposlenici Fakulteta, suradnici i studenti koji u svome radu koriste računala. Fakultet zadržava pravo promjene korisničkog imena u skladu sa zahtjevom ili preporukama Akademske zajednice (CARNet-a).
- Administratori su dužni zaporke tehnički ugraditi u sve sustave koji to omogućavaju.

Članak 23.

Pravila za korištenje zaporki

- Korisničko ime sastoji se od prezimena korisnika bez naših znakova (š, đ, č, ć, i ž pišu se kao s, d, c, c i z). U slučaju istih prezimena, ispred korisničkog imena se stavlja jedno ili dva slova imena.
- Minimalna dužina zaporke je šest znakova
- Za zaporku se ne smiju koristiti riječi iz rječnika, preporuča se izmiješati mala i velika slova s brojevima, ne preporuča se korištenje imena bliskih osoba, ljubimaca, datume rođenja i sl.
- 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. Ukoliko korisnik zaboravi zaporku, administrator će mu omogućiti da unese novu.

Članak 24.

Administriranje zaporki

- Na računalima koja spadaju u zonu visokog rizika administratori su dužni konfigurirati sustav na taj način da se korisnički račun zaključa nakon tri neuspjela pokušaja prijave.
- Administratori su po potrebi dužni konfigurirati autentikaciju 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 jesu li korisničke zaporke u skladu s navedenim pravilima.

Članak 25.

Nepridržavanje

- Korisnici koji se ne pridržavaju navedenih pravila ugrožavaju sigurnost informacijskog sustava.
- Fakultet je obvezan odgojno djelovati i obrazovati korisnike u kreiranju sigurnih zaporki.
- 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.

Članak 26.

Pravilnik o korištenju elektroničke pošte

- Izgled pojedinačne korisničke adrese elektronske pošte može, ali ne mora, biti po principima korisničkog imena za pristup računalima. Svako korisničko ime za elektronsku poštu u nastavku ima ekstenziju " @vef.hr ", što određuje poslužiteljsko računalo. Korisnici mogu rabiti prividna imena (alias) koja u sebi sadrže jedinstveni oblik adrese.
- pravila za korištenje e-maila odnose se na sve zaposlene, vanjske suradnike, i studente koji imaju otvoren korisnički račun na poslužitelju Veterinarski fakultet.

Članak 27.

Procedura za dodjelu e-mail adrese

- Pri zapošljavanju novog djelatnika, rukovodilac zatraži od administratora poslužitelja elektroničke pošte otvaranje korisničkog računa.
- Pri prestanku radnog odnosa, rukovodilac je dužan najkasnije u roku od sedam dana zatražiti zatvaranje korisničkog računa.
- Zaposlenicima se otvara korisnički račun radi obavljanja posla.
- Studenti imaju pravo besplatnog korištenja e-maila za vrijeme trajanja studija. Nakon odlaska s Fakulteta njihov se korisnički račun zatvara.

Članak 28.

Pravila prihvatljivog korištenja

- Poruke koje su dio poslovnog procesa treba arhivirati i čuvati propisani vremenski period kao i dokumente na papiru.
- Svaka napisana poruka smatra se dokumentom, te na taj način podliježe propisima o autorskom pravu i intelektualnom vlasništvu. Osobne poruke ne smiju se proslijediti dalje bez dozvole autora, odnosno pošiljatelja

- Službenu e-mail adresu ne smije se koristiti za slanje uvredljivih, omalovažavajućih poruka, ili za seksualno uznemiravanje.
- Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme.
- Sve poruke pregledat će automatski aplikacija koja otkriva viruse. Ako poruka zadrži virus, ne će biti isporučena, a pošiljatelj i primatelj će biti o tome obaviješteni. Poruka će provesti određeno vrijeme u karanteni, odakle ju je moguće na zahtjev primatelja izvući. Nakon određenog vremena, obično mjesec dana, poruka se briše iz karantene kako bi se oslobodio prostor na disku.
- Fakultet zadržava pravo filtriranja poruka s namjerom da se zaustavi spam.
- U slučaju istrage uzrokovane mogućim sigurnosnim incidentom, sigurnosni tim može pregledavati kompletan sadržaj diska, pa time i e-mail poruke.

Članak 29.

Nepridržavanje

- Protiv korisnika koji ne poštuju ova pravila Fakultet može pokrenuti stegovni postupak. U slučaju ponovljenih težih prekršaja, korisniku se može zatvoriti korisnički račun i uskratiti pravo korištenja servisa elektroničke pošte.

Članak 30.

Pravilnik o antivirusnoj zaštiti

Zaštita od virusa obvezna je i provodi se na tri razine:

- na poslužiteljima elektroničke pošte;
- na internim poslužiteljima gdje se stavlja centralna instalacija;
- na svakom osobnom računalu korisnika.
- Administratori su dužni instalirati protuvirusne programe na sva korisnička računala i konfigurirati ih tako da se izmjene u bazi virusa i u konfiguraciji automatski propagiraju s centralne instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika.
- Korisnici ne smiju samovoljno isključiti protuvirusnu zaštitu na svome računalu. Ukoliko iz nekog razloga moraju privremeno zaustaviti protuvirusni program, korisnici moraju obavijestiti sistem inženjera.

Članak 31.

Nepridržavanje

- Korisnik koji samovoljno isključi protuvirusnu zaštitu na svom računalu, te na taj način izazove štetu, bit će stegovno kažnjen.

Članak 32.

Pravilnik o zaštiti od neželjene pošte (spama)

Pravila za administratore:

- Administratori poslužitelja elektroničke pošte dužni su konfigurirati računala na taj način da se što više neželjenih poruka zaustavi.
- Definirati ulazni filter koji će prilikom primanja poruke konzultirati 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 ne će se primati.
- Podesiti poslužitelj da poruke koje su obilježene kao spam sprema na određeno vrijeme u karantenu.
- Krajnjem korisniku prepustiti uključivanje bodovanja i konfiguriranje preusmjeravanja označenih poruka. Poruke dobivaju bodove koji ukazuju na vjerojatnost da se radi o spamu. Kako nije uvijek moguće pouzdano definirati što je spam, ovakva zaštita mora biti uvjetna (na korisničkoj razini).
- Informatičar zadužen za sigurnost treba obučiti korisnike i pomagati im pri kreiranju filtera za obilježavanje, odvajanje ili uništavanje neželjenih poruka.

Članak 33.

Pravila za korisnike

- Korisnici ne smiju slati masovne poruke, bez obzira na njihov sadržaj.
- Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći računalnu opremu koja pripada Fakultetu.

Članak 34.

Nepridržavanje

- Protiv korisnika koji se ne pridržavaju pravila prihvatljivog korištenja i šalju masovne neželjene poruke bit će pokrenut stegovni postupak.

Članak 35.

Pravilnik o rješavanju sigurnosnih incidenata

Prijava incidenta

- 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.

- Fakultet treba izraditi i održavati kontakt listu osoba kojima se prijavljuju problemi u radu računala i servisa, te obrazac za prijavu incidenta. Kontakt listu treba podijeliti svim zaposlenima i objaviti je na internim web stranicama Fakulteta.
- Svaki incident se dokumentira. Uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac s opisom incidenta i poduzetih mjera pri rješavanju problema.
- 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 36.

Procedure za rješavanje incidenata

- 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).
- Daljnja istraga može se provesti samo ako je prijavljena Povjerenstvu za sigurnost koje je uspostavljeno sigurnosnom politikom Fakulteta, uz poštivanje sljedećih pravila:
    - Istragu provodi jedna osoba, ali uz prisutnost svjedoka kako bi se omogućilo svjedočenje o poduzetim radnjama.
    - Informacijski sustav sačuvati u zatečenom stanju, odnosno da se ne učine izmjene koje bi otežale ili onemogućile dijagnosticiranje.
    - Napraviti kopiju zatečenog stanja (npr. na traku, CD...), po mogućnosti na takav način da se ne izmijene atributi datoteka (na Unixu naredbom dd).
    - Dokumentirati svaku radnju tako da se ponavljanjem zabilježenih akcija može rekonstruirati tijek istrage.
    - Napisati izvještaj, kako bi u slučaju potrebe mogao poslužiti 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.
    - Fakultet može objavljivati statističke podatke o sigurnosnim incidentima, bez otkrivanja povjerljivih i osobnih informacija.

Članak 37.

Sankcije

- 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 podatcima.
- Ukoliko je incident izazvao zaposlenik vanjske tvrke, Fakultet može zatražiti od vanjske tvrtke da ga ukloni s popisa osoba ovlaštenih za obavljanje poslova u ustavovi. U slučaju teže povrede pravila sigurnosne politike, Fakultet može raskinuti ugovor s vanjskom tvrtkom.

Članak 38.

Pravilnik o upravljanju povjerljivim informacijama

Klasifikacija informacija

Klasificiranje povjerljivih informacija uređeno je Zakonom o zaštiti tajnosti podataka objavljenim u Narodnim novinama br. 114/01.

- Poslovna tajna su informacije koje imaju komercijalnu vrijednost i čije bi otkrivanje moglo nanijeti štetne posljedice Fakultetu ili njegovim poslovnim partnerima (ugovori, financijski izvještaji, planovi, rezultati istraživanja itd.).
- Profesionalna tajna odnosi se na zanimanja poput liječnika, svećenika i odvjetnika, no može se primijeniti i na zaposlene koji u svom radu dolaze u dodir s podatcima o drugim ljudima, poput zaposlenih u referadi, osoba koje unose podatke u baze podataka o studentima ili sistem administratora poslužitelja koji u nekim situacijama može doći u dodir s podatcima koji pripadaju korisnicima računala.
- Dokumenti koji izvana dolaze na Fakultet s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će Fakultet proizvesti kao odgovor. U tom slučaju može se koristiti neka od kategorija tajnosti koje su rezervirane za tijela državne uprave (službena, državna ili vojna tajna).
- Dokumenti koji se smatraju povjerljivima moraju biti jasno označeni isticanjem vrste i stupnja tajnosti.
- Javnima se smatraju sve informacije koje nisu označene kao povjerljive. Izuzetak su osobne informacije, za koje se podrazumijeva da su povjerljive i ne treba ih posebno označavati.
- Pravila za čuvanje povjerljivosti odnose se na informacije bez obzira na to u kom su obliku: na papiru, u elektroničkom obliku, zabilježene ili usmeno prenesene, ili su objekti poput maketa, slika itd.

Članak 39.

Raspodjela odgovornosti

- Za klasificiranje povjerljivih informacija zadužen je u rukovoditelj Fakulteta, koji će izraditi popis osoba koje imaju pravo proglasiti podatke tajnima, te popis osoba koje imaju pristup povjerljivim podatcima.
- Pravila za čuvanje povjerljivih informacija odnose se na sve zaposlenike Fakulteta i vanjske suradnike koji dolaze u doticaj s osjetljivim podatcima. Obveza čuvanja povjerljivosti ne prestaje s prestankom radnog odnosa.

Članak 40.

Čuvanje povjerljivih informacija

- Povjerljive informacije, tiskane na papiru ili u elektroničkom obliku, snimljene na neki medij za pohranu podataka, čuvaju se u zaključanim metalnim, vatrootpornim ormarima, u prostorijama u koje je ograničen pristup.
- Pristup povjerljivim informacijama regulira se izradom popisa zaposlenika koji imaju ovlasti, te bilježenjem vremena izdavanja i vraćanja dokumenata, kako bi se u svakom trenutku znalo gdje se oni nalaze.

Članak 41.

Informacije o zaposlenicima

Informacije o zaposlenima koje se smatraju «javnima» mogu biti objavljene na web stranicama Fakulteta.

Članak 42.

Javnim informacijama smatraju se:
- ime i prezime i titula,
- posao koji zaposlenik obavlja,
- broj telefona na poslu,
- službena e-mail adresa.
- Na upite o zaposlenicima davat će se samo informacije objavljene na internim web stranicama.
- Informacije o zaposlenima ne smiju se davati bez suglasnosti osobe kojoj podatci pripadaju (npr. adresa stana, broj privatnog telefona, podaci o primanjima, porezu, osiguranju itd.).
- Povjerljive informacije u načelu se ne daju telefonom jer se sugovornik može lažno predstaviti.
- Ukoliko se sugovornik predstavlja kao službena osoba koja ima pravo pristupa povjerljivim podatcima, zapisuje se ime i prezime te osobe, naziv institucije kojoj pripada i broj telefona s kojeg zove. Nakon provjere istinitosti tih podataka zaposlenik će se posavjetovati s upravom i ukoliko dobije odobrenje nazvati službenu osobu i odgovoriti na pitanja.

Članak 43.

Prenošenje povjerljivih informacija

- Informacije koje su klasificirane kao povjerljive zahtijevaju posebne procedure pri slanju i prenošenju.
- Povjerljive informacije ne šalju se običnom poštom, već kurirskom. Na odredištu se predaju u ruke osobi kojoj su upućeni, što se potvrđuje potpisom.

- Povjerljive informacije koje se šalju elektronički, na primjer kao poruke elektroničke pošte, moraju se slati kriptirane.

Članak 44.

Kopiranje povjerljivih informacija

- Za kopiranje povjerljivih informacija treba zatražiti dozvolu vlasnika informacije.
- Povjerljivi dokumenti koji izvana dođu na Fakultet ne smiju se kopirati bez izričite dozvole pošiljatelja.
- Dokumenti koji pripadaju Fakultetu smiju se kopirati samo uz dozvolu osobe koja ih je proglasila povjerljivim, odnosno uprave. Kopija se numerira i o njenom izdavanju vodi se evidencija kao i za original s kojeg je proizvedena.
- Osoblje koje poslužuje uređaje za kopiranje treba obučiti i obvezati da odbiju kopiranje povjerljivih dokumenata ukoliko nije ispoštovana propisana procedura.

Članak 45.

Uništavanje povjerljivih informacija

- Mediji koji sadrže povjerljive informacije ne bacaju se, već se uništavaju metodom koja osigurava da se trajno i pouzdano uništi sadržaj (spaljivanjem, usitnjavanjem, prešanjem).
- Ukoliko se zastarjela i rashodovana računalna oprema daje na korištenje trećoj strani, obvezno je uništavanje podataka s diskova posebnim programom koji nepovratno prebriše sadržaj diska.

Članak 46.

Nepridržavanje

- Zaposlenici i suradnici koji dolaze u dodir s klasificiranim informacijama potpisuju izjavu o čuvanju povjerljivosti informacija.
- Protiv zaposlenika koji ne poštuju pravila o čuvanju povjerljivih informacija bit će pokrenut stegovni postupa, a može ih se premjestiti na drugo radno mjesto na kojem ne će dolaziti u dodir s povjerljivim podatcima.
- S vanjskim suradnicima za koje se ustanovi da otkrivaju povjerljive informacije razvrgnuti će se ugovor. Fakultet treba već u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.

Članak 47.

Pravilnik stupa na snagu osmi dan od dana objave na oglasnoj ploči Veterinarskoga fakulteta.

Klasa: 012-03/06-41/1
Ur. broj: 61-01/139-06-1

Dekanica

Prof. dr. sc. Ljiljana Pinter

Pravilnik je objavljen_____te je stupio na snagu _____ .

Tajnik