VELEUČILIŠTE VELIKA GORICA

Pravilnik o računalnoj informacijskoj sigurnosti

(Sigurnosna politika informacijskih sustava)

Velika Gorica, 2013.

Na temelju članka 38. Statuta Veleučilišta Velika Gorica Stručno vijeće Veleučilišta Velika Gorica na na svojoj 8. sjednici održanoj 19. rujna 2013.godine donosi

PRAVILNIK
O RAČUNALNOJ INFORMACIJSKOJ SIGURNOSTI

I. Uvod

Članak 1.

Ovaj pravilnik donesen je sa svrhom da:

- Definira prihvatljive načine ponašanja u svezi korištenja računalnog informacijskog sustava Veleučilišta Velika Gorica (u daljnjem tekstu – Veleučilište).
- Raspodjeli zadatke i odgovornosti nadležnih osoba.
- Zaštiti investiciju Veleučilišta u računalni informacijski sustav.
- Zaštiti informacije i podatke koji se u sustavu kreiraju, prenose, pohranjuju i obrađuju.
- Propiše sankcije u slučaju nepridržavanja odredbi ovog pravilnika.

Sastavni dio ovog pravilnika su i slijedeće procedure:

- „Procedura o prihvatljivim načinima uporabe lokalne mreže i javne računalne mreže Interneta“, br. IS-1;
- „Procedura za uporabu sustava elektroničke pošte“, br. IS-2;
- „Procedura za uporabu prijenosnih računala“, br. IS-3;
- „Procedura za objavljivanje informacija putem računalne mreže“, br. IS-4,
- „Procedura za uporabu poslovnih sustava“, br. IS-5;
- „Procedura za upravljanje povjerljivim i važnim informacijama“, br. IS-6;
- „Procedura o rješavanju sigurnosnih incidenata“, br. IS-7;
- „Procedura o antivirusnoj zaštiti i zaštiti od spama“, br. IS-8;
- „Procedura o rukovanju zaporkama“, br. IS-9
- „Procedura za uporabu prostorija podatkovnog centra“, br. IS-10.

Članak 2.

Korisnik je svaka osoba koja koristi informatičku opremu i informacijski sustav u vlasništvu ili na korištenju u Veleučilištu.

Glavni korisnik je korisnik koji je odgovoran za funkcioniranje nekog informacijskog podsustava Veleučilišta. (npr. voditelj Odsjeka za računovodstvene i knjigovodstvene poslove je glavni korisnik informacijskog podsustava za knjigovodstvene i računovodstvene poslove). Glavne korisnike za pojedine informatičke podsustave određuje svojom odlukom Dekan Veleučilišta.

Menadžer informatičke sigurnosti (u daljnjem tekstu Menadžer IT sigurnosti) je najodgovornija osoba za informatičku sigurnost u Veleučilištu.

Davatelji usluga su profesionalci koji se brinu o radu računala, mreže i informacijskih sustava. U Veleučilištu su to sistem inženjeri i IT profesionalci zaposlenici Odsjeka za informatičku potporu, te vanjski IT profesionalci s kojima je sklopljen ugovor o suradnji na održavanju informatičkog sustava u Veleučilištu. Oni odgovaraju za ispravnost i neprekidnost rada informacijskog sustava.

Povjerenstvo za sigurnost informacijskog sustava formira Veleučilište s ciljem kvalitetnijeg sveukupnog upravljanja informacijskom sigurnošću Veleučilišta.

Podatkovni centar (data centar) je odvojeni prostor za smještaj računalne opreme koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskog sustava, ili sadrži povjerljive informacije u tom sustavu.

Poslovni informacijski sustav je računalni sustav koji obuhvaća jedan ili više sustava za računalnu potporu poslovnih procesa (računovodstvo i knjigovodstvo, kadrovski poslovi, upravljanje studentima, i slično).

II. Opseg primjene ovog pravilnika

Članak 3.

Ovaj pravilnik odnosi se na zaposlenike, vanjske suradnike i studente (u daljnjem tekstu termin korisnik odnosit će se na ove osobe koje koriste informatički sustav Veleučilišta) kojima se dopušta uporaba računalnog informacijskog sustava Veleučilišta Velika Gorica (u daljnjem tekstu Veleučilište).

Pravilnik obuhvaća računalni informacijski sustav Veleučilišta i sve sadržaje koji se prenose, pohranjuju i obrađuju u tom sustavu, sadržaje pohranjene na svim osobnim računalima u

vlasništvu Veleučilišta, kao i sve poslužitelje koji su u administrativnoj domeni ili vlasništvu Veleučilišta.

III. Odgovornost

Članak 4.

Za primjenu ovog Pravilnika i korištenje informatičke opreme u vlasništvu Veleučilišta najodgovorniji je voditelj Odsjeka za informatičku potporu ili druga osoba određena posebnom odlukom Dekana Veleučilišta (u daljnjem tekstu – Menadžer IT sigurnosti).

Odsjek za informatičku potporu odgovoran je za:

- administriranje i održavanje sigurnosti računalnog informacijskog sustava što uključuje materiju koju uređuje ovaj pravilnik, i sve pridružene procedure,
- razvijanje i održavanje pisanih standarda i procedura kojima se osigurava primjena i pridržavanje odredbi ovog Pravilnika i procedura,
- pružanje odgovarajuće podrške korisnicima u ispunjavanju njihove obveze u odnosu na ovaj Pravilnik i pripadajuće procedure.

Čelnici ustrojbenih cjelina obvezni su u svojim ustrojbenim cjelinama osigurati da svi korisnici budu upoznati s ovim Pravilnikom, te da ga se pridržavaju.

Svi korisnici obvezni su proučiti i primjenjivati ovaj Pravilnik kao i njemu pridružene procedure iz članka 1. ovog Pravilnika.

Članak 5.

Veleučilište štiti svoju računalnu opremu, sklopovlje, programsku podršku, podatke i dokumentaciju od zlouporabe, krađe, neovlaštene uporabe i upliva okoliša.

Za sigurnost računalnog informacijskog sustava Veleučilišta odgovorni su korisnici i Menadžer IT sigurnosti, svaki u svom dijelu odgovornosti propisane ovim Pravilnikom.

Povjerljivost i integritet podataka pohranjenih na računalnom informacijskom sustavu Veleučilišta moraju biti zaštićeni sustavom kontrole pristupa kako bi se osiguralo da samo ovlašteni korisnici imaju pristup potrebnim informacijama. Taj pristup treba biti ograničen na samo one informacijske sustave i mogućnosti koje su korisniku nužne za njegove poslovne aktivnosti.

Članak 6.

Menadžer IT sigurnosti odgovoran je da sva kritična računalna oprema bude priključena na izvore neprekidnog napajanja, a ostala oprema da bude zaštićena prednaponskom zaštitom.

Odsjek za informatičku potporu odgovoran je za sve instalacije, odspajanja, promjene i premještanje računalne opreme. Korisnici ne smiju samostalno poduzimati takve radnje (ovo se ne odnosi na prijenosna računala za koja je početnu konfiguraciju i priključenje u sustav obavio Odsjek za informatičku potporu.

Članak 7.

Korisnici, glede informacijske sigurnosti, su obvezni pridržavati se slijedećih uputa:

- Mediji s podacima i programskom podrškom (diskete, diskovi, trake i ostali mediji) za vrijeme kada nisu u upotrebi, ne smiju biti izloženi na lako dostupnim mjestima neovlaštenim osobama;
- Mediji koji sadrže povjerljive i važne podatke trebaju biti čuvani u adekvatnim zaključanim kasama ili metalnim ormarima;
- Podatkovni mediji trebaju se čuvati podalje od nepovoljnih utjecaja okoliša kao što su toplina, direktno sunčevo svjetlo, vlaga i elektromagnetska polja i slično;
- Utjecaji okoliša kao što su dim, hrana, tekućine, previsoka ili preniska vlažnost, previsoke ili preniske temperature moraju se izbjegavati;
- Prijenosna računala i drugu prijenosnu opremu koju rabi više korisnika, korisnici ne smiju iznositi izvan Veleučilišta bez odobrenja Menadžera IT sigurnosti;
- Korisnici se trebaju s pažnjom odnositi prema povjerenoj im računalnoj opremi;
- Korisnik će se smatrati odgovornim za štete nastale na računalnoj opremi ako su nastale uslijed nepažnje ili nepravilne uporabe.

IV. Povjerenstvo za sigurnost informacijskog sustava

Članak 8.

Povjerenstvo ustanovljava Dekan svojom odlukom, a na prijedlog Menadžera IT sigurnosti.

Povjerenstvo je načelno u sastavu: Menadžer za IT sigurnost, predstavnik uprave, predstavnika vanjskog davatelja usluge (ako postoji) i Glavni korisnici.

Povjerenstvo predsjedava Menadžer za IT sigurnost.

Članak 9.

Povjerenstvo prima izvještaje o sigurnosnoj situaciji i predlaže mjere za njeno poboljšanje, uključujući nabavu opreme, organizaciju obrazovanja korisnika i specijalista.

Povjerenstvo pokreće i daje odobrenje za provođenje istrage u slučaju incidenata.

Povjerenstvo podnosi izvještaj o stanju sigurnosti upravi Veleučilišta, te se zalaže za donošenje konkretnih mjera, nabavu potrebne opreme, ulaganje u obrazovanje specijalista, ali i običnih korisnika.

V. Administriranje korisnika

Članak 10.

Odsjek za informatičku potporu odgovoran je za administraciju kontrole pristupa u računalni informacijski sustav, što uključuje dodavanje, brisanje i promjene prava pristupa korisnicima.

Administracija korisnika se temelji na zahtjevima:

- Odsjeka za studentska pitanja za studente i
- prodekana i čelnika ustrojbene cjeline u čijoj je organizacijskoj nadležnosti korisnik.

Zahtjev se dostavlja putem obrasca „*Zahtjev za administraciju korisnika*“ koji je sastavni dio ovog Pravilnika.

U slučaju hitnosti, brisanja i zabrane prava pristupa mogu se izvršiti i na usmeni zahtjev nadležnog čelnika ustrojbene cjeline, nakon čega mora slijediti i pismeni zahtjev kao potvrda.

Članak 11.

Odsjek za studentska pitanja, obvezan je za svakog studenta koji gubi status studenta završetkom ili prekidom studija, najkasnije 15 dana od gubitka statusa studenta, dostaviti Odsjeku za informatičku potporu zahtjev za brisanje korisnika.

Prodekan za nastavnu djelatnost obvezan je za svakog nastavnika i suradnika kojem po bilo kojem osnovu prestaje nastavna djelatnost u Veleučilištu, a najkasnije 15 dana od prekida suradnje ili od zadnje nastavne obveze na Veleučilištu, dostaviti Odsjeku za informatičku djelatnost zahtjev za brisanje korisnika.

Odjel za marketing, opće i kadrovske poslove prestanak radnog odnosa zaposlenika, mora prijaviti Odsjeku za informatičku potporu istodobno s odlukom o prestanku radnog odnosa po bilo kojoj zakonskoj osnovi kako bi njihova pristupna prava i zaporke bili opozvani ili izmijenjeni.

Članak 12.

Korisnik osobnog računala može putem obrasca *„Zahtjev za administraciju korisnika“,* a za potrebe korištenja istog osobnog računala od strane druge osobe (demonstrator, vanjski suradnik i dr.), zatražiti otvaranje lokalnog korisničkog računa na računalu koje koristi.

VI. Administriranje računalne opreme

Članak 13.

Svako računalo mora imati imenovanog administratora, koji odgovara za instalaciju i konfiguraciju softvera.

Menadžer IT sigurnosti može naprednim korisnicima odobriti da sami administriraju svoje osobno računalo.

Članak 14.

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 administratori su dužni posvetiti opremi koja obavlja ključne funkcije ili sadrži vrijedne i povjerljive informacije koje treba štiti od neovlaštenog pristupa (npr. serveri, mrežna oprema i slično).

Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla.

Članak 15.

Administratori su dužni prijaviti incidente Menadžeru za IT sigurnost, te pomoći pri istrazi i uklanjanju problema. Incidente treba dokumentirati kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti.

Članak 16.

Administratorska prava na računalima koja koriste više osoba mogu imati samo osobe Odsjeka za informatičku potporu.

Administratorska prava na osobnim računalima za osobne potrebe mogu biti dodijeljena i samom korisniku, ukoliko Menadžer IT sigurnosti procijeni da je on stručno sposoban samostalno administrirati računalo na osobnom korištenju, a na svim ostalim osobnim računalima administratorska prava mogu imati samo osobe Odsjeka za informatičku potporu.

VII. Upravljanje računalnom mrežom

Članak 17.

Upravljanje računalnom mrežom u nadležnosti je isključivo Odsjeka za informatičku potporu i ugovorene vanjske davatelje usluge održavanja računalne mreže.

Članak 18.

Odsjek za informatičku potporu mora ažurno voditi dokumentaciju o cjelokupnoj računalnoj mreži Veleučilišta, koja se obvezno treba čuvati u metalnom ormaru (kasi) u vrijeme kad se ne koristi.

U koliko je dokumentacija o računalnoj mreži u digitalnom formatu, Menadžer IT sigurnosti je obvezan propisati način sigurnog korištenja za davatelje usluge.

Odsjek za informatičku potporu mora u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala.

Članak 19.

Veleučilište treba na prijedlog Menadžera IT sigurnosti propisati pravila za spajanje na računalnu žičnu i bežičnu mrežu Veleučilišta gostujućih računala, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri i serviseri.

VIII. Zaporke i pristupni računi

Članak 20.

Zabranjuje se korištenje grupnih i univerzalnih pristupnih računa za pristup računalima i računalnim sustavima.

Svaka osoba obvezno mora pristupiti računalnom sustavu i računalima Veleučilišta isključivo vlastitim pristupnim računom.

Izuzetno, Menadžer IT sigurnosti može na pismeno traženje Dekana ili Prodekana za nastavnu djelatnost odobriti korisniku korištenje pristupnog računa druge osobe za pronalaženje i otklanjanje nepravilnosti rada sustava, o čemu treba sačiniti pisani dokument.

Nakon završetka radnji iz stavka 3 ovog članka, obavezno treba promijeniti zaporku toga pristupnog računa.

IX. Postupak sa zaporkama

Članak 21.

Korisnik:

- je odgovoran za sve računalne transakcije učinjene korištenjem dodijeljenog mu prijavnog imena i zaporke,
- ne smije njemu dodijeljene zaporke otkriti drugim osobama,
- treba odmah promijeniti svoju zaporku, ako posumnja da ju je netko drugi saznao,
- ne smije bilježiti zaporke na lako dostupnom mjestu,
- treba često mijenjati zaporke, a obvezno nakon 90 dana korištenja,
- treba koristit zaporke koje nije lako pogoditi,
- treba se odjaviti iz informacijskog sustava kada napušta radno mjesto.

Članak 22.

Menadžer IT sigurnosti obvezan je pohraniti sve administratorske zaporke u adekvatni metalni ormar (kasu) koju treba uvijek držati zaključanu.

Pohranjene zaporke trebaju biti u svaka u zasebnoj zapečaćenoj kuverti, na kojoj treba pisati za koji je računalni sustav ili računalnu opremu, te datum kad je zadnji puta ažurirana.

Menadžer IT sigurnosti obvezan je redovito nakon svake promijene ažurirati pohranjene zaporke.

X. Računalni virusi

Članak 23.

Računalni virusi i drugi zlоćudnih programi (u daljnjem tekstu - virusi) su programi načinjeni sa svrhom da čine neovlaštene promjene na podacima i aplikacijama, stoga računalni virusi mogu nanijeti štetu Veleučilištu.

Pri tome je važno znati:

- računalne viruse jednostavnije je spriječiti nego liječiti,
- obrana protiv računalnih virusa uključuje zaštitu od neovlaštenog pristupa računalnim resursima, uporabu samo provjerenih izvora podataka i programske zaštite, te održavanje ažurnim sustava za detekciju i uklanjanje virusa.

Članak 24.

Uprava Veleučilišta u pogledu zaštite od računalnih virusa je obvezna u svom proračunu redovito osiguravati dostatna financijska sredstva za nabavku i održavanje programske i sklopovske opreme za zaštitu od njih.

Članak 25.

Odsjek za informatičku potporu obvezan je:

- instalirati i održavati odgovarajuće antivirusne programe na svim računalima u vlasništvu ili u najmu Veleučilišta,
- reagirati na svaki napad virusa, uništiti svaki detektirani virus i dokumentirati incident,
- dati uputu korisnicima o postupanju glede detektiranog virusa.

Članak 26.

Obveze korisnika glede računalnih virusa su:

- Korisnici ne smiju svjesno unijeti računalni virus u računalni sustav Veleučilišta;
- Korisnici trebaju izbjegavati internetske stranice na kojima se pružaju nelegalne usluge, piratske kopije računalnih programa i audio/video sadržaja, te pornografiju.

- Korisnici ne smiju na računalima Veleučilišta rabiti podatkovne medije nepoznatog porijekla i sadržaja;
- Korisnik treba sam ili uz pomoć stručne osobe antivirusnim programom, odobrenim od strane Odsjeka za informatičku potporu, pregledati medije koji se unose prije njihove upotrebe;
- Ukoliko korisnik posumnja da je njegovo računalo zaraženo virusom ili da antivirusna zaštita nije aktivna ili ažurna, korisnik mora računalo odmah isključiti i prijaviti zapažanje Odsjeku za informatičku potporu.

XI. Intelektualno vlasništvo i licenčna prava

Članak 27.

Obveza je Veleučilišta i svih njenih zaposlenika da poštuju zakone i propise o zaštiti intelektualnog vlasništva.

Veleučilište je obvezno koristi programsku podršku na temelju valjanih licenčnih prava.

Veleučilište programsku podršku i pripadajuću dokumentaciju koja nije u vlasništvu Veleučilišta, nema pravo umnožavati i distribuirati bez dopuštenja proizvođača ili autora, osim za potrebe stvaranja sigurnosne kopije.

Na računalima u vlasništvu Veleučilišta ne smije se bez odobrenja Menadžera IT sigurnosti koristiti programska podrška nabavljena privatno, bilo kupnjom ili donacijom. Legalnost licenci donirane programske podrške utvrđuje se Ugovorom o donaciji.

Članak 28.

Odsjek za informatičku potporu mora:

- održavati ažuran popis programskih licenci u vlasništvu Veleučilišta,
- čuvati licenčne ugovore ili uvjete korištenja programske potpore,
- periodički, metodom slučajnog odabira pregledati računala u vlasništvu Veleučilišta radi provjere uporabe samo legalne programska podrške.

Članak 29.

Korisnici ne smiju:

- koristiti programsku podršku na način koji nije u skladu s licenčnim pravima proizvođača,
- instalirati aplikacije koje nije odobrio Odsjek za informatičku potporu na računala u vlasništvu Veleučilišta;
- na računala u vlasništvu Veleučilišta instalirati programsku podršku koja nije licencirana ili nije u vlasništvu Veleučilišta,
- kopirati programsku podršku bez prethodnog odobrenja Odsjeka za informatičku potporu,
- preuzimati programsku podršku s Interneta bez prethodnog odobrenja Odsjeka za informatičku potporu.

Članak 30.

Korisnici moraju biti svjesni da kršenje Zakona o intelektualnom vlasništvu može izložiti Veleučilište i pojedinca prekršitelja kaznenom postupku kojeg pokreću nadležna državna tijela neovisno od namjera Veleučilišta,

Korisnici trebaju obavijestiti Odsjek za informatičku potporu o svim zlouporabama programske podrške ili informatičke opreme Veleučilišta o kojima imaju saznanja.

XII. Fizička zaštita

Članak 31.

Računalna oprema koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskog sustava Veleučilišta, ili sadrži povjerljive informacije, fizički se odvaja u prostor (podatkovni centar) u koji je ulaz dozvoljen samo ovlaštenim osobama.

Članak 32.

Ulazak osoba u podatkovni centar treba biti strogo kontroliran. Dekana ili Menadžera IT sigurnosti odobravaju popis osoba koje mogu ulaziti u pojedine dijelove podatkovnog centra.

Ulazak osoba u podatkovni centar osoba koje nisu na popisu iz stavka 2. ovog članka može biti jednokratno pismeno odobren od strane Menadžera IT sigurnosti u slučajevima

održavanja opreme u podatkovnom centru od strane vanjskih davatelja usluge (servisera) ili drugih neodložnih poslova, pri čemu takve osobe borave u podatkovnom centru uz nazočnost nekog od zaposlenika Odsjeka za informatičku potporu.

Ulazak u osoba iz stavka 3. ovog članka obvezno se evidentira u dnevniku ulaska osoba u podatkovni centar.

Članak 33.

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.

Podatkovni centar treba biti zaštićen od poplava, požara i slično, te treba poduzeti mjere da se oprema i informacije zaštite, te da se osigura što brži oporavak.

U podatkovnom centru i bliskom prostoru oko njega zabranjeno je držanje zapaljive i eksplozivne stvari i materijale.

Članak 34.

Ukoliko Veleučilište prepušta vanjskoj tvrtki održavanje opreme i aplikacija s povjerljivim podacima, menadžer IT sigurnosti odobrava popis osoba vanjske tvrtke koje će dolaziti u prostorije podatkovnog centra Veleučilišta radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti Veleučilište.

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

XIII. Fizička sigurnost opreme

Članak 35.

U prostorijama Veleučilišta nalazi se informatička oprema u vlasništvu Veleučilišta, oprema u najmu drugih vlasnika i oprema CARNeta, koja je dana na korištenje Veleučilištu.

Voditelj Odsjeka za informatičku potporu (ili druga osoba po odluci Dekana) odgovorna je za održavanje ažurnog popis sve računalne opreme, s popisom ugrađenih glavnih modula komponenti, inventarskim brojevima itd.

Veleučilište treba brinuti jednako o svoj opremi kojom raspolaže, bez obzira na to tko je njezin vlasnik manirom dobrog gospodara čuvajući je od oštećivanja i otuđenja.

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

XIV. Neprekidnost poslovanja

Članak 36.

Kako bi se sačuvali podaci u slučaju nezgoda, poput kvarova na sklopovlju, požara, ili ljudskih grešaka, 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.

Izrada kopija iz stavka 1. ovog članka *on-line* preko zasebne računalne mreže ili Interneta obvezno se treba izvoditi primjenom adekvatnog sustava kriptiranja podataka u prijenosu.

Članak 37.

Veleučilište treba osigurati povremeno uvježbavanje oporavka i uporabljivosti rezervnih kopija.

Uvježbavanje se obvezno obavlja u laboratorijskim uvjetima na rezervnoj opremi i programskoj potpori koja ne služi za produkciju.

XV. Procedure

Uporaba lokalne računalna mreže i Interneta

Članak 38.

Uporaba Interneta regulirana je posebnom *„**Procedura o prihvatljivim načinim uporabe lokalne mreže i javne računalne mreže Interneta“ br. IS-1**,* koja je pridružena ovom Pravilniku i njegov je sastavni dio te s njime čini cjelinu sigurnosti računalnog informacijskog sustava Veleučilišta.

Članak 39.

Svrha donošenja ove procedure je odrediti smjernice, postupke i zahtjeve za osiguranje prihvatljivih načina uporabe lokalne računalne mreže Veleučilišta kao i javne računalne mreže - Interneta, te zaštitu informacija i opreme Veleučilišta od zlouporaba korištenjem lokane mreže i Interneta.

Članak 40.

Procedura odnosi se na zaposlenike, studente, vanjske suradnike i sve druge osobe kojima se dopušta uporaba računalnog informacijskog sustava Veleučilišta korištenjem lokalne mreže i Interneta.

Članak 41.

Odgovornost za primjenu ove procedure imaju sistem administratori sustava (zaposleni ili vanjski po ugovoru), čelnici ustrojbenih cjelina, te svi korisnici.

Od svih korisnika se očekuje da budu upoznati s odredbama ove procedure, te da ih u svakodnevnom radu poštuju.

Članak 42.

Odgovornost i obveze sistem administratora ogleda se u:

- uspostavljanju i održavanju sigurnosnih pravila i standarda te davanju korisnicima Veleučilišta tehničku potporu pri uporabi lokalne mreže i Interneta,
- organiziranju i provođenju reakcije na moguće krizne situacije u računalnom sustavu Veleučilišta (zaraza računalnim virusom, napad hakera i sl.),
- provođenju periodičke procjene sigurnosnih rizika na svim produkcijskim sustavima koji su u njegovoj odgovornosti,
- provjeri sigurnosnih mjera implementiranih na tim sustavima i utvrđivanju da li odgovaraju razini osjetljivosti u njima pohranjenih informacija,
- osiguranju pristupna prava pojedinih korisnika na najmanjoj razini potrebnoj za njihov rad,
- nadziranju uporabe Interneta, detektiranju mogućih kršenja odredbi ove procedure, te izvještavanja o tim pojavama Menadžera IT sigurnosti.

Članak 43.

Čelnici ustrojbenih cjelina moraju osigurati da:

- svi korisnici u njihovim ustrojbenim cjelinama budu upoznati s ovom procedurom, te da se pridržavaju njezinih odredbi,

Članak 44.

Korisnici računalnog sustava Veleučilišta moraju:

- poznavati i primjenjivati odredbe ove procedure,
- ne dozvoliti neovlaštenim pojedincima pristup u lokalnu mrežu Veleučilišta i odatle javnu računalnu mrežu Internet,
- održavati tajnost uporabe svojih pristupnih zaporki za mrežne usluge i zaštitit ih od nenamjernog otkrivanja drugim osobama,
- menadžeru za IT sigurnost ili administratoru sustava prijaviti svaku pojavu za koju se čini da narušava sigurnost informacijskog sustava Veleučilišta pri korištenju lokalne mreže ili Interneta (virusne zaraze, neobjašnjive transakcije, nedostajuće podatke, neovlašteno ili zabranjeno skidanje programa i audio/video sadržaja i slično,
- pristupati samo podacima i funkcijama za koje su slijedom redovnih poslovnih aktivnosti ovlašteni,
- tražiti ovlaštenje od nadležnih osoba za sve aktivnosti koje izlaze iz okvira korisnikovih redovnih poslovnih aktivnosti, posebno aktivnosti razmjene podataka s osobama i sustavima izvan Veleučilišta,

Uporaba elektroničke pošte

Članak 45.

Uporaba elektroničke pošte regulirana je posebnom procedurom „***Procedura za uporabu sustava elektroničke pošte", br. IS-2****,* koja je pridružena ovom Pravilniku i njegov je sastavni dio te s njime čini cjelinu sigurnosti računalnog informacijskog sustava Veleučilišta.

Svrha donošenja ove procedure je davanje smjernice poslovanja, postupke i zahtjeve za osiguranje prihvatljivih načina uporabe sustava elektroničke pošte Veleučilišta, te zaštitu informacija i resursa Veleučilišta od zlouporaba korištenjem elektroničke pošte.

Članak 46.

Ova procedura odnosi se na sve zaposlenike, vanjske suradnike, studente, gostujuće profesore i studente i sve druge osobe kojima je dopuštena uporaba računalnog informacijskog sustava Veleučilišta.

Procedura obuhvaća sustav elektroničke pošte i sve poruke elektroničke pošte smještene na osobna računala u vlasništvu Veleučilišta kao i sve poslužitelje elektroničke pošte u administrativnoj domeni ili vlasništvu Veleučilišta.

Procedura se odnosi i na sva računala u vlasništvu Veleučilišta, priključena u računalnu mrežu Veleučilišta ili samostalna računala priključena u Internet pomoću drugih veza.

Članak 47.

Odgovornost za primjenu ove procedure imaju sistem administratori sustava (zaposleni ili vanjski po ugovoru), čelnici ustrojbenih cjelina, te svi korisnici.

Članak 48.

Administrator sustava mora:

- uspostaviti i održavati sigurnosna pravila i standarde te korisnicima Veleučilišta davati tehničku podršku pri uporabi sustava elektroničke pošte,
- nadzirati rad i uporabu sustava elektroničke pošte, detektirati moguća kršenja odredbi ove procedure, te o tim pojavama izvijestiti menadžera za IT sigurnost.

Članak 49.

Čelnici ustrojbenih cjelina moraju osigurati da svi njihovi korisnici elektroničke pošte budu upoznati s ovom procedurom, te da se pridržavaju njezinih odredbi.

Uporaba prijenosnih računala

Članak 50.

Uporaba prijenosnih računala regulirana je posebnom procedurom ***„Procedura o uporabi prijenosnih računala“ br. IS-3****,* koja je pridružena ovom Pravilniku i njegov je sastavni dio te s njime čini cjelinu sigurnosti računalnog informacijskog sustava Veleučilišta.

Svrha donošenja ove procedure je definiranje pravila korištenja prijenosnih računala u vlasništvu Veleučilišta i prijenosnih računala drugih vlasnika koja se priključuju u lokalnu mrežu Veleučilišta.

Članak 51.

Ova procedura odnosi se na sve zaposlenike Veleučilišta, poslovne suradnike koji koriste privatno ili službeno prijenosno računalo kao sredstvo rada na Veleučilištu.

Objavljivanje informacija putem računalne mreže

Članak 52.

Objavljivanje informacija putem računalne mreže i Interneta regulirano je posebnom procedurom *„**Procedura za objavljivanje informacija putem računalne mreže“ br. IS-4***, koja je pridružena ovom Pravilniku i njegov je sastavni dio te s njime čini cjelinu sigurnosti računalnog informacijskog sustava Veleučilišta.

Svrha donošenja ove procedure je davanje smjernice za poslovanje, postupke i zahtjeve za osiguranjem prihvatljivih načina uporabe računalne mreže i Interneta za interno i javno objavljivanje informacija na mrežnim stranicama veleučilišta, mrežnim stranicama Veleučilišta na društvenim mrežama, uključujući procedure za administriranje web stranica intraneta i Interneta i mrežnih stranica na društvenim mrežama, te zaštitu informacija i resursa Veleučilišta od zlouporaba.

Članak 53.

Ova procedura odnosi se na zaposlenike, studente, vanjske suradnike, gostujuće studente i sve druge osobe kojima je dopuštena uporaba računalnog informacijskog sustava Veleučilišta za objavljivanje informacija na mrežnim stranicama Veleučilišta.

Procedura obuhvaća sustav za administriranje mrežnih stranica intraneta (Pretinac), mrežnih stranica javne mreže, mrežne stranica Veleučilišta na društvenim mrežama, te sve poslužitelje koji su dio ovog sustava, a u administrativnoj su domeni ili vlasništvu Veleučilišta.

Članak 54.

Dekan svojom odlukom formira Uredništvo javnih mrežnih stranica Veleučilišta, koje je odgovorno za objavljivanje informacija na mrežnim im stranicama Veleučilišta.

Uredništvo čine glavni urednik, administratori mrežnih stranica i druge osobe imenovane od Uprave Veleučilišta.

Članak 55.

Uredništvo mrežnih stranica:

- definira i objavljuje upute za objavu informacija na mrežnim stranicama,
- određuje strukturu informacija na mrežnim stranicama, te definira stupnjeve ovlasti za rad sa sustavom,
- predlaže i nadzire vizualnu i sadržajnu ujednačenost objavljenih informacija,
- nadzire korektnost objavljenih informacija te korektnost uporabe sustava od strane korisnika,
- objavljuje informacije po zahtjevima i odobrenju Uprave Veleučilišta, odnosno, po zahtjevima ovlaštenih čelnika ustrojbenih cjelina Veleučilišta,
- prati posjećenost mrežnim stranicama s ciljem unapređenja kvalitete rada Veleučilišta.

Članak 56.

Obveze administratora mrežnih stranica su:

- davanje ovlaštenja korisnicima za pristup pojedinim dijelovima sustava,
- koordinacija aktivnosti vezane uz ispravnost funkcioniranja tehničke podrške sustava,
- briga o statistikama administriranja i posjećenosti mrežnih stranica koje se koriste u svrhu unapređenja sustava,
- nadziranje ispravnost funkcioniranja sustava,
- u suradnji s tehničkim osobljem predlaganje i provođenje sigurnosnih mjera koje osiguravaju zaštitu od neovlaštenog korištenja podataka i neovlaštenog objavljivanja informacija.

Uporaba poslovnih sustava

Članak 57.

Uporaba poslovnih sustava regulirana je posebnom procedurom ***„Procedura za uporabu poslovnih sustava“, br. IS-5****,* koja je pridružena ovom Pravilniku i njegov je sastavni dio te s njime čini cjelinu sigurnosti računalnog informacijskog sustava Veleučilišta.

Svrha donošenja ove procedure definiranje pravila i ovlasti korištenja poslovnih sustava.

Članak 58.

Procedura se odnosi na sve zaposlenike Veleučilišta koji u svom svakodnevnom poslu koriste poslovne sustave.

Upravljanje povjerljivim i važnim podacima

Članak 59.

Upravljanje povjerljivim podacima i informacijama regulirano je posebnom procedurom „***Procedura za upravljanje povjerljivim i važnim podacima" br. IS-6***, koja je pridružena ovom Pravilniku i njegov je sastavni dio te s njime čini cjelinu sigurnosti računalnog informacijskog sustava Veleučilišta.

Svrha donošenja ove procedure je zaštiti povjerljive računalne podatke kojima raspolaže bilo koji segment Veleučilišta od neovlaštenog njihovog dohvaćanja trećih osoba.

Članak 60.

Ova procedura se odnosi na sve čelnike ustrojbenih cjelina i na sve korisnike koji na bilo koji način raspolažu ili dolaze u kontakt s povjerljivim informacijama.

Čelnici ustrojbenih cjelina obvezni su voditi brigu o ograničenoj dostupnosti povjerljivih informacija i podataka za to nadležnim korisnicima u njihovoj ustrojbenoj cjelini, a posebno da:

- korisnici brišu osjetljive (povjerljive) informacije sa svojih diskova i drugih vanjskih memorijskih komponenti kad im ti podaci više nisu potrebni za rad,
- korisnici snimaju i pohranjuju svoje zaštitne kopije važnih informacija u skladu s razinom važnosti informacija,
- korisnici kojima prestaje radni odnos na Veleučilištu prođu postupak razduživanja informatičke opreme i pohranjenih povjerljivih i važnih podataka prije napuštanja Veleučilišta.
- osiguraju da podaci pod korisnikovom kontrolom budu pravilno zaštićeni, u skladu s razinom osjetljivosti informacija,
- korisnici snimaju zaštitne kopije važnih podataka onoliko često koliko sami smatraju razumnim za razinu važnosti informacija.

Rješavanje sigurnosnih incidenata

Članak 61.

Svrha je ove procedure je da ustanovi obavezu prijavljivanja sigurnosnih incidenata, te da razradi procedure za provođenje istrage.

Članak 62.

Svaki zaposlenik, student ili suradnik Veleučilišta dužan je prijavljivati sigurnosne incidente, poput usporenog rada servisa, nemogućnosti pristupa, gubitka ili neovlaštene izmjene podataka, pojave virusa itd.

Članak 63.

Menadžer IT sigurnosti 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 mrežnim stranicama Veleučilišta.

Članak 64.

Svaki incident se dokumentira. Uz obrazac za prijavu incidenta, dokumentacija sadrži i obrazac s opisom incidenta i poduzetih mjera pri rješavanju problema.

Članak 65.

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 incidente obavezno se prijavljuju CARNetovom CERT-u, preko obrasca na web stranici www.cert.hr

Antivirusna zaštita i zaštita od spama

Članak 66.

Antivirusna zaštita i zaštita od spama regulirana je posebnom procedurom ***„Procedura o antivirusnoj zaštiti i zaštiti od spama“, br. IS-8;***, koja je pridružena ovom Pravilniku i njegov je sastavni dio te s njime čini cjelinu sigurnosti računalnog informacijskog sustava Veleučilišta.

Svrha donošenja ove procedura je osigurati i provoditi sustavnu zaštitu od zloćudnih programa (virusa) i neželjenih elektroničkih poruka (spama).

Članak 67.

Zaštita od virusa ne smije više biti stvar osobnog izbora, već obaveza Veleučilišta, administratora računala i svakog korisnika.

Zaštitu od virusa i obvezno se provoditi na više razina:

- na poslužiteljima elektroničke pošte,
- na svim poslužiteljima poslovnih i javnih servisa,
- na svakom osobnom računalu.

Članak 68.

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 sa centralne instalacije na korisnička računala u lokalnoj mreži, bez aktivnog sudjelovanja korisnika.

Članak 69.

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 70.

Administratori poslužitelja elektroničke pošte dužni su konfigurirati računala na taj način da se što više neželjenih poruka zaustavi i preusmjeri u mapu neželjenih poruka.

Korisnicima treba omogućiti da samostalno odrede koje poruke jesu ili nisu spam za njih.

Stručno osoblje Odsjeka za informatičku potporu dužno je obučiti korisnike i pomagati im u kreiranju filtera za obilježavanje, odvajanje ili uništavanje neželjenih poruka.

Rukovanje zaporkama

Članak 71.

Pravila rukovanja zaporkama regulirana je posebnom procedurom „**Procedura o rukovanju zaporkama**“, br. IS-9, koja je pridružena ovom Pravilniku i njegov je sastavni dio te s njime čini cjelinu sigurnosti računalnog informacijskog sustava Veleučilišta.

Svrha donošenja ove procedure je osigurati sigurno korištenje i čuvanje zaporki na svim razinama i za sve informacijske sustave u uporabi na Veleučilištu.

Članak 72.

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

Članak 73.

U kreiranju zaporki svi korisnici su dužni poštivati odredbe ove procedure, posebno u:

- minimalnoj duljini zaporke,
- izbjegavanju korištenja riječi iz javno dostupnih rječnika,
- kombinaciji velikih i malih slova, znakova interpunkcija i znamenki u zaporkama,
- izbjegavanju korištenja imena bliskih osoba, ljubimaca, karakterističnih datuma i njihovih kombinacija,
- trajanju zaporke.

Članak 74.

Korisnici su odgovorni za svoju zaporku i ni u kom je slučaju ne smiju otkriti, čak ni administratorima sustava.

Uporabu prostorija podatkovnog centra

Članak 75.

Pravila i nadzor korištenja sobe s poslužiteljima regulirana je posebnom procedurom ***„Procedura za uporabu prostorija podatkovnog centra, br. IS-7“*** , koja je pridružena ovom Pravilniku i njegov je sastavni dio te s njime čini cjelinu sigurnosti računalnog informacijskog sustava Veleučilišta.

Svrha donošenja ove Procedure je osigurati siguran pristup i zaštiti od neovlaštenog pristupa u prostor podatkovnog centra Veleučilišta.

Članak 76.

Menadžer IT sigurnosti treba definirati sigurnosne zone podatkovnog centra, te odrediti pravila ulaska u pojedine zone.

XVI. Prekršaji i sankcije

Članak 77.

Svi korisnici računalnog sustava Veleučilišta dužni su pridržavati se odredbi ovog Pravilnika, procedura sadržanih u njemu kao i svih drugih internih odluka koje reguliraju korištenje računalnog sustava i informatičke opreme.

Članak 78.

Kršenje odredbi ovog Pravilnika i sadržanih procedura može korisnika izložiti opozivu prava uporabe računalnog sustava Veleučilišta, te pokretanju stegovnog postupka sve do prestanka ugovora o radu iz razloga uvjetovanog iskrivljenim ponašanjem radnika ili prestanka drugih primjenjivih ugovora.

Članak 79.

Sankcija za učinjenu povredu odnosno korištenje računalnog informacijskog sustava Veleučilišta protivno odredbama ovog Pravilnika ovisit će o vrsti i veličini prekršaja, zatim da li je prekršajem uzrokovana pravna, materijalna ili kakva druga šteta, te radi li se o prvom ili ponovljenom prekršaju.

Članak 80.

Sankcije donosi Dekan na prijedlog Povjerenstva za stegovnu odgovornost.

XVII. Završne i prijelazne odredbe

Članak 81.

Ovaj Pravilnik, zajedno sa pripadajućim procedurama, stupa na snagu danom donošenja.

Članak 82.

Prilagodni period za potpunu primjenu ovog Pravilnika traje šest (6) mjeseci od dana donošenja.

Klasa: 602-04/13-14/01 Dekan

Ur.Broj: 238/31-132-051-13-785

Velika Gorica, 19. rujan 2013. mr.sc. Ivan Toth, v.pred.