VELEUČILIŠTE VELIKA GORICA

Pravilnik o računalnoj informacijskoj sigurnosti

(Sigurnosna politika informacijskog sustava)

rujan, 2013

Na temelju članka 38. Statuta Veleučilišta Velika Gorica Stručno vijeće Veleučilišta Velika Gorica na svojoj sjednici od _____. g., donijelo je

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 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 podacima“, br. IS-6;
- „Procedura za rješavanje sigurnosnih incidenata“, br. IS-7;
- „Procedura za antivirusnu zaštitu i zaštitu od spama“, br. IS-8;
- „Procedura za rukovanje zaporkama“, br. IS-9
- „Procedura za uporabu prostorija podatkovnog centra“, br. IS-10
- „Procedura sigurnosne pohrane podataka“, br. IS-11

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 zloćudnih 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 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:

Ur.Broj:

Dekan:

Ivan Toth

IS- 1
PROCEDURA O PRIHVATLJIVIM NAČINIMA UPORABE LOKALNE I JAVNE RAČUNALNE MREŽE INTERNETA

VLASNIŠTVO

1. Sve informacije koje prolaze kroz računalnu mrežu Veleučilišta, a koje nisu specifično identificirane kao vlasništvo drugih pravnih i fizičkih osoba, bit će tretirane na isti način kao da su vlasništvo Veleučilišta.

2. Politika je Veleučilišta da se ne dopušta neovlašten pristup, odavanje, umnažanje, mijenjanje, preusmjeravanje, uništavanje, nepropisna uporaba i otuđivanje takvih informacija.

3. Nadalje, politika je Veleučilišta da štiti informacije koje pripadaju drugim pravnim ili fizičkim osobama, a povjerene su Veleučilištu u povjerenju i u skladu s primjenjivim ugovorima i standardima.

ODGOVORNA UPORABA

4. Veleučilište dopušta korisnicima da koriste javnu računalnu mrežu- Internet i istražuje njen informacijski prostor za obavljanje znanstveno- nastavnih i poslovnih aktivnosti.

5. Informacijski sustav Veleučilišta svojom konfiguracijom onemogućava korisnicima pristup svim internetskim sadržajima koji se ne mogu kvalificirati prihvatljivim za obavljanje znanstveno- nastavnih i poslovnih aktivnosti. Pristup blokiranim sadržajima može se omogućiti pojedinim korisnicima na njihov zahtjev i uz suglasnost Uprave.

PRIJENOS INFORMACIJA

6. Svi podaci i programska podrška dopremljena u računalni sustav Veleučilišta iz izvora izvan računalnog sustava Veleučilišta moraju biti pregledani programima za detekciju računalnih virusa i ostalih vrsta malicioznog programskog koda, prije nego se počnu koristiti unutar računalnog sustava Veleučilišta.

7. Korisnicima informacijskog sustava Veleučilišta, može se dodijeliti limitirani mrežni diskovni prostor koji je dio mrežnog sustava za pohranu podataka, a čija je veličina ograničena fizičkom veličinom diskova u sustavu. Podaci pohranjeni na dodijeljeni

diskovni prostor se sigurnosno kopiraju, te su na taj način zaštićeni. Na dodijeljenom diskovnom prostoru dopušteno je pohranjivati isključivo datoteke iz nastavnog, stručnog ili znanstvenog područja.

8. Kad god izvor programske podrške nije potpuno pouzdan, dopremljenu programsku podršku treba isprobati na posebnom ispitnom računalu koje nije spojeno u računalnu mrežu Veleučilišta kako bi se ograničila šteta u slučaju postojanja virusa ili nekih drugih vrsta malicioznog programskog koda.

9. Na Internetu ne postoji kontrola kvalitete, odnosno načina na koji sadržaji nastaju kao i zbog raznolikosti izvora iz kojih dolaze, mnoge informacije mogu biti netočne i zastarjele. Stoga sve informacije koje dolaze iz neprovjerenih izvora i nepouzdanih internetskih izvora treba smatrati neprovjerenim, sve dok se ne dobije potvrda o točnosti informacija iz drugog, nezavisnog izvora.

10. Bez primjene posebnih sustava autentikacije na Internetu se je jednostavno predstavljati kao druga osoba. Stoga se kontaktima načinjenim putem Interneta ne smiju otkrivati interne informacije koje nisu izričito označene kao dozvoljene za javnu uporabu.

11. Sadržaje koji su vlasništvo Veleučilišta (programska podrška, poslovni podaci, dokumenti, poruke elektroničke pošte, i sl.) korisnici ne smiju pohranjivati na računala koja su dostupna za anonimni pristup s javne računalne mreže, osim sadržaja za koje postoji odobrenje ovlaštene osobe.

12. Svi podaci i sadržaji javno dostupni na računalima u vlasništvu Veleučilišta, koja funkcioniraju kao dio lokalne ili javne mreže biti će redovito pregledavani od strane odsjeka za informatičku potporu kako bi se spriječila ilegalna i anonimna razmjena sadržaja protivnih odredbama ove procedure. Primjeri ovakvih sadržaja uključuju ilegalne kopije programske podrške, ukradene zaporke i brojeve kreditnih kartica, pornografske materijale, slike, glazbu i slično.

13. Korisnicima je zabranjeno sudjelovanje u stvaranju, razmjeni i uporabi takvih sadržaja na bilo koji način.

ZAŠTITA INFORMACIJA

14. Povjerljive informacije u vlasništvu Veleučilišta ne smiju se prenositi nesigurnim kanalima putem javne računalne mreže ako prethodno nisu kriptirane odobrenim

metodama. Uza svu poslovnu dokumentaciju ovo se odnosi i na prijavne zaporke i druge informacije koji mogu poslužiti za neovlašteno pribavljanje pristupa u računalni sustav Veleučilišta.

15. Korisnici, kojima to Dekan Veleučilišta odobri, mogu pristupati računalnim resursima lokalne mreže Veleučilišta s udaljenih lokacija preko Interneta samo preko sigurnog i kriptiranog komunikacijskog kanala (VPN-a). Djelatnici Odsjeka za informatičku potporu nadležni su za instalaciju programske potpore za VPN. Menadžer IT sigurnosti mora ažurno voditi popise svih korisnika resursa LAN mreže na daljinu s najvažnijim podacima.

16. Radi zaštite intelektualnog vlasništva, poslovnih podataka i informacija Veleučilišta sva dokumentacija, programska podrška, dopisi, poruke i drugi oblici internih podataka i informacija ne smiju se predati, proslijediti ili na bilo koji drugi način otuđiti i prenijeti osobama izvan Veleučilišta za bilo koje druge potrebe osim akademskih i poslovnih potreba izričito odobrenih od strane nositelja intelektualnog vlasništva ili od strane Dekana za slučaj poslovnih podataka i informacija.

17. Razmjena podataka između Veleučilišta i drugih pravnih i fizičkih osoba ne smije se provoditi bez prethodno sklopljenog ugovora kojim se ugovaraju uvjeti razmjene te načini rukovanja zaštite podataka.

POŠTIVANJE PRAVILA PRIVATNOSTI

18. Veleučilište poštuje prava korisnika uključujući i pravo privatnosti u razumnoj mjeri. Korisnici računalnog sustava Veleučilišta trebaju biti svjesni da njihove komunikacije nisu automatski zaštićene od uvida trećih strana. Sadržaje koje smatraju privatnima ne trebaju slati nesigurnim kanalima preko javne mreže kakva je Internet.

19. Dekan Veleučilišta pridržava pravo da u bilo koje vrijeme, bez prethodne najave, izda nalog da se određenom korisniku izvrši pregled elektroničke pošte, mapa i datoteke i ostalih informacija pohranjenih na računalima u vlasništvu Veleučilišta. Kontrola i pregledavanje provodi se u svrhu podupiranja primjene ove i srodnih procedura, pomoći u internim istražnim radnjama i olakšanju poslovanja računalnim sustavom.

20. Veleučilište dozvoljava uporabu računala u vlasništvu Veleučilišta u privatne svrhe ali na način da se svi privatni podaci korisnika računala nalaze pohranjeni u direktoriju naziva „privatno“ koji se nalazi unutar direktorija „moji dokumenti“. Prigodom

prestanka radnog odnosa po bilo kojoj osnovi, korisniku će se omogućiti da preuzme sve dokumente u navedenom direktoriju.

JAVNO PREDSTAVLJANJE

21. Prilikom sudjelovanja u diskusijama, razgovorima i ostalim načinima osobne interakcije u Internetu korisnici smiju iskazati svoju povezanost s Veleučilištem, bilo izričitim tekstom bilo implicitno, na primjer adresom elektroničke pošte.

22. U oba slučaja, korisnici moraju jasno ukazati na to da su iznesena mišljenja njihova osobna i ne predstavljaju stajalište Veleučilišta.

23. Dodatno, kad god je istaknuta veza korisnika s Veleučilištem, korisnik se mora pridržavati pravila pristojnog ponašanja u komunikaciji putem Interneta.

24. Bez odobrenja Dekana Veleučilišta korisnici ne smiju javno, putem Interneta obznanjivati interne informacije Veleučilišta koje mogu utjecati na javnu sliku institucije.

KONTROLA PRISTUPA

25. Bez prethodnog odobrenja administratora sustava, korisnici ne smiju samostalno uspostavljati određene tipove dvosmjernih internetskih veza koje bi osobama izvan Veleučilišta omogućile ostvarivanje neovlaštenog pristupa u računalni sustav Veleučilišta. Ovo uključuje uspostavljanje raznih računalnih servisa i protokola.

IZVJEŠTAVANJE O SIGURNOSNIM PROBLEMIMA

26. Ukoliko korisnik opravdano sumnja, ili zna da su osjetljive informacije Veleučilišta izgubljene, ukradene ili obznanjene neovlaštenim osobama, mora odmah izvijestiti menadžera IT sigurnosti ili administratora sustava.

27. Ukoliko korisnik opravdano sumnja, ili zna da se računalni sustav Veleučilišta neovlašteno rabi, ili da se rabi u nedopuštene svrhe, mora odmah izvijestiti menadžera IT sigurnosti ili administratora sustava.

28. Ukoliko korisnik opravdano sumnja, ili zna da su zaporke ili drugi kontrolni mehanizmi pristupa izgubljeni, ukradeni ili obznanjeni neovlaštenim osobama, mora odmah izvijestiti menadžera IT sigurnosti ili administratora sustava.

29. Ukoliko korisnik opravdano sumnja, ili zna da je u računalni sustav Veleučilišta unesen računalni virus, mora odmah izvijestiti menadžera IT sigurnosti ili administratora sustava.

30. Korisnici ne smiju iskušavati (pokušavati probiti ili zaobići) sigurnosne mehanizme računalnog sustava Veleučilišta. Takvi pokušaji aktiviraju alarme i nepotrebno troše resurse za praćenje ilegalne aktivnosti.

31. Određene specifičnosti sigurnosne problematike računalnog informacijskog sustava predstavljaju poslovnu tajnu, svi korisnici moraju uvažavati tu činjenicu.

IS- 2
PROCEDURA ZA UPORABU SUSTAVA ELEKTRONIČKE POŠTE

OVLAŠTENA UPORABA

1. Kao sredstvo unapređivanja produktivnosti, Veleučilište potiče poslovnu uporabu elektroničkih komunikacija (elektronička pošta, Internet, sobne i grupne videokonferencije, online chat, sustave za udaljeno učenje itd.). Svaka poruka elektroničke pošte može se smatrati autorskim djelom, dakle pripada osobi koja ju je poslala. Stoga za prosljeđivanje tuđe poruke morate tražiti dozvolu njezina autora. Prilozi koji se šalju uz elektroničke poruke mogu sadržavati autorski zaštićene informacije, na primjer glazbu, filmove, članke itd. Primajući i šaljući takve sadržaje korisnici mogu biti izloženi tužbi ne samo sebe, već i Veleučilišta.

2. Sustav elektroničke pošte Veleučilišta u pravilu se mora koristiti samo u znanstvene, istraživačke i poslovne svrhe. Privatne poruke dozvoljene su u umjerenoj količini, ukoliko to ne ometa rad.

3. Pišući poruke e-pošte korisnici moraju biti svjesni da ne predstavljaju samo sebe, već i ustanovu za koju rade.

4. Pridržavajući se pravila pristojnog ponašanja na Internetu, korisnici službenu e-mail adresu ne smiju koristiti za slanje uvredljivih, omalovažavajućih poruka, ili za seksualno uznemiravanje.

5. Nije dozvoljeno slanje lančanih poruka kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme. Svaka napisana poruka smatra se dokumentom, te na taj način podliježe propisima o autorskom pravu i intelektualnom vlasništvu. Poruke koje su poslane osobno jednom korisniku, taj korisnik nema pravo proslijediti dalje bez dozvole autora, odnosno pošiljatelja.

6. Sve poruke automatski će pregledati aplikacija koja otkriva viruse. Ako pošiljka sadrži virus, neće biti isporučena, a primatelj će o tome biti obaviješten. Poruka će neko vrijeme provesti u karanteni.

7. Poruke koje su dio poslovnog procesa treba arhivirati i čuvati propisani vremenski period kao i dokumente na papiru.

8. Korisnicima nije dopušteno presretati i pregledavati, niti pomagati u presretanju i pregledavanju sadržaja elektroničke pošte drugih korisnika.

9. Korisnicima je zabranjena uporaba elektroničke pošte za privatne poslovne aktivnosti, dobrotvorne akcije i zabavne aktivnosti.

10. Uporaba elektroničke pošte ne smije stvarati ni privid niti stvarnost nepropisne uporabe.

OSNOVNE KORISNIČKE OVLASTI

11. Osnovne ovlasti korisnika u sustavu elektroničke pošte postavljaju se na onaj minimum koji je dovoljan za obavljanje njegove poslovne aktivnosti. Osim u slučajevima opasnosti i sustavnih poruka administratora sustava, slanje poruka svim korisnicima informacijskog sustava Veleučilišta nije dopušteno bez prethodnog odobrenja Uprave.

RAZDVAJANJE KORISNIKA

12. Sustav elektroničke pošte konfiguriran je tako da se razdvaja pošta različitih korisnika. Svakom korisniku elektroničke pošte dodijeljen je poštanski pretinac kojemu on pristupa putem jedinstvenog korisničkog imena i pripadajuće zaporke. Svaki korisnik treba za elektroničku komunikaciju koristiti samo svoj poštanski pretinac. Uporaba tuđeg poštanskog pretinca nije dopuštena, osim u slučajevima poslovnih zajedničkih pretinaca ustrojbenih ili poslovnih cjelina.

13. Korisniku može biti dopušteno korištenje poštanskih pretinaca vezanih uz posebne korisničke račune i adrese e-pošte (npr., grupne adrese, adrese konferencija…) temeljem odluke čelnika ustrojbene cjeline, a po odobrenju Dekana.

ODGOVORNOST KORISNIKA

14. Korisnik je dužan čuvati tajnost zaporke i ne otkrivati je drugim osobama, kako bi se spriječila zloporaba njegovog poštanskog pretinca. Ukoliko posumnja da je njegova zaporka kompromitirana, korisnik treba hitno obavijestiti administratora sustava. Otkrivanje zaporke drugoj osobi povlači sa sobom odgovornost korisnika za akcije koje ta osoba može pod uzeti korištenjem njegove zaporke.

POVJERLJIVOST ELEKTRONIČKE POŠTE NIJE ZAJAMČENA

15. Korisnici se podsjećaju da se u sustavu elektroničke pošte Veleučilišta u redovnom radu ne koristi enkripcija sadržaja. Ukoliko je elektroničkom poštom potrebno slati povjerljive sadržaje, prije slanja na te sadržaje treba primijeniti metode enkripcijske zaštite. U svezi s time, treba se obratiti administratoru sustava.

POŠTIVANJE PRAVA PRIVATNOSTI

16. Veleučilište poštuje pravo svojih korisnika uključujući i pravo privatnosti u razumnoj mjeri, ali privatnost e-pošte nije zajamčena.

17. U posebnim slučajevima, kad postoji opravdana sumnja u kršenje odredbi ove procedure, radi zaštite sustava elektroničke pošte i po zahtjevu ovlaštenih državnih ustanova, Veleučilište može dopustiti povremeno presretanje i pregledavanje sadržaja elektroničke pošte svojih korisnika.

18. U slijed prethodno navedenih razloga, Veleučilište ne može jamčiti privatnost sadržaja e-pošte u svom sustavu. Korisnici trebaju biti svjesni da poruke e-pošte mogu bez njihova znanja, ovisno o tehnologiji, biti prosljeđivane, presretane, tiskane ili pohranjivane od drugih osoba.

19. Veleučilište zadržava pravo filtriranja poruka s namjerom da se zaustave nepoželjne poruke e-pošte - tzv. spam.

STATISTIČKI PODACI

20. U skladu s općeprihvaćenom poslovnom praksom, Veleučilište prikuplja statističke podatke o uporabi sustava elektroničke pošte. Statistički podaci mogu obuhvatiti adrese pošiljatelja i primatelja, veličine poruka, nazive i veličine privitaka, datum i vrijeme slanja ili primanja; i ostale podatke; navedeno omogućuje administratoru sustava održavanje i razvijanje sustava elektroničke pošte.

SLUČAJNI UVID

21. Pri rješavanju problema komunikacije, administrator sustava nekad trebaju uvid u sadržaj poruka elektroničke pošte pojedinačnog korisnika. Obično se radi o probnim porukama beznačajnog sadržaja, a korisnika se o tome obavijesti i zatraži njegov pristanak.

22. Administrator sustava ne smije pregledava li sadržaj elektroničke pošte drugih korisnika iz osobne radoznalosti, niti dopustiti uvid u sadržaj elektroničke pošte trećim o sobama koje za to nemaju potrebna ovlaštenja Uprave.

PROSLJEĐIVANJE PORUKA

23. Neke informacije su namijenjene određenim pojedincima i ni su podobne za opću distribuciju. U tom smislu korisnici sustava elektroničke pošte trebaju biti oprezni pri prosljeđivanju informacija. Informacije povjerljivog sadržaja za Veleučilište ne smiju se slati na adrese izvan računalnog sustava Veleučilišta.

BRISANJE ELEKTRONIČKIH PORUKA

24. Poruke koje više nisu bitne za poslovne potrebe korisnik treba brisati iz svog poštanskog pretinca na poslužitelju e-pošte ili ih premjestiti u lokalnu arhivu e-pošte na osobnom računalu. Poruke pohranjene na zaštitnim kopijama (*backup*) bit će i zbrisane nakon isteka definiranog vremena čuvanja.

25. Ukoliko je u tijeku neka istražna akcija, uzrokovana mogućim sigurnosnim incidentom, pokrenuta od Uprave Veleučilišta ili od strane ovlaštenih državnih ustanova, sve poruke elektroničke pošte relevantne za tu istražnu akciju neće biti brisane do izričite naredbe Uprave ili sistem administratora.

KONTAKT

26. Pitanja u vezi s ovom procedurom mogu se uputiti administratoru sustava.

IS- 3
PROCEDURA ZA UPORABU PRIJENOSNIH RAČUNALA

OPĆENITO

1. Sva prijenosna računala kupljena od Veleučilišta vlasništvo su Veleučilišta. Svaki korisnik koji duži prijenosno računalo odgovoran je za njegovu sigurnost.

2. Za korištenje prijenosnih računala vrijede sve sigurnosne procedure kao i za stolna računala, kako je navedeno u proceduri pri prihvatljivim načinima korištenja lokalne računalne mreže i javne računalne mreže-Interneta, br. IS-1.

3. U slučaju nestanka prijenosnog računala korisnik je o tome dužan odmah obavijestiti Menadžera za IT sigurnost, te ga upoznati sa svim relevantnim podacima vezanim uz nestanak prijenosnog računala.

SIGURNOSNI STANDARDI PRI KORIŠTENJU PRIJENOSNIH RAČUNALA

1. Prijenosno računalo ne smije se: ostaviti na mjestu vidljivom kroz prozor vozila, ostaviti u kabini vozila bez nadzora lako dostupno potencijalnim kradljivcima već mora biti smješteno u prtljažnik automobila i nevidljivo izvana.

2. Korisnik je odgovoran za poduzimanje svih potrebnih mjera radi minimiziranja rizika od gubitka ili krađe prijenosnog računala.

3. Prijenosno računalo mora biti dodatno zaštićeno vatrozidom (*firewall*), kako bi se spriječili neovlašteni upadi u računalo kada se ono koristi unutar druge mreže koja nije sastavni dio mreže Veleučilišta (Internet i sl.).

IS- 4
PROCEDURA ZA OBJAVLJIVANJE INFORMACIJA PUTEM RAČUNALNE MREŽE

VLASNIŠTVO

1. Pod sustavom za objavljivanje informacija podrazumijevaju se web poslužitelji i web stranice, kao i slični računalni sustavi koji omogućavaju dostup do informacija s daljine. U Veleučilištu egzistiraju bilo u vlasništvu ili u najmu slijedeći takvi sustavi:
    a. web poslužitelj s oficijelnim mrežnim web stranicama Veleučilišta,
    b. web poslužitelj e-učenja s adekvatnim programskim rješenjem za e-učenje (Gaudeamus),
    c. web poslužitelj i web aplikacija za upravljanje nastavnim procesom i studentima (Pretinac),
    d. web poslužitelj i web stranice za posebne događaje, tematske stranice i nastavničke stranice.
    e. web stranice Veleučilišta na društvenim mrežama (Facebook, Twiter, ...).
2. Veleučilište potiče poslovnu uporabu intraneta i javne mreže kao sredstva za unapređivanje produktivnosti u svrhu pružanja informacija zaposlenicima, studentima i širokoj javnosti.
3. Svi sadržaji objavljeni ili preneseni posredstvom sustava iz točke 1., uključujući zaštitne kopije, smatraju se vlasništvom Veleučilišta.

OVLAŠTENA UPORABA

4. Sustavi iz točke 1. se koristi u edukativne, znanstveno-istraživačke i poslovne svrhe.
5. Pristupajući sustavu i postavljajući sadržaje putem sustava, korisnici moraju biti svjesni da ne predstavljaju samo sebe, već i ustanovu za koju rade.
6. Na intranet i javnu mrežu korisnici ne smiju postavljati netočne i neprovjerene informacije.

7. Pridržavajući se pravila pristojnog ponašanja na Internetu, korisnici ne smiju koristiti sustav za postavljanje uvredljivih ili omalovažavajućih poruka, niti za seksualno uznemiravanje.

8. Nije dozvoljeno postavljanje sadržaja kojima se opterećuju mrežni resursi i ljudima oduzima radno vrijeme.

9. Svaki tekst i datoteka postavljena putem ovih sustava smatra se dokumentom, te na taj način podliježe propisima o autorskom pravu i intelektualnom vlasništvu.

10. Korisnici su pri objavljivanju informacija dužni poštivati intelektualno pravo vlasništva dokumenata drugih autora.

11. Korisnicima je zabranjena uporaba sustava za privatne poslovne aktivnosti. Dobrotvorne akcije i zabavne aktivnosti osim po izričitom odobrenju Dekana ili urednika.

12. Korisnici ne smiju iskušavati (pokušavati probiti ili zaobići) sigurnosne mehanizme sustava. Takvi pokušaji najstrože će se sankcionirati.

OSNOVNE KORISNIČKE OVLASTI

13. Osnovne ovlasti korisnika u sustavu postavljaju se na minimum dovoljan za obavljanje njegove poslovne aktivnosti. To se prvenstveno odnosi na pristup administraciji osobnih stranica te stranica pripadajućih kolegija.

14. Po izričitom odobrenju urednika korisniku se može dodijeliti šire ovlaštenje za korištenje sustava.

15. Korisnik se pri pristupanju sustavu identificira svojim korisničkim imenom i zaporkom. Prilikom preuzimanja korisničkog imena i zaporke, korisnika se upoznaje s ovom procedurom, a svojim potpisom na izjavu o preuzimanju korisničkog imena i zaporke, korisnik potvrđuje da je s njome upoznat i da će se pridržavati njenih odredbi.

16. Za pristup sustavu korisnik je dužan koristiti isključivo osobno korisničko ime i zaporku, a uporaba tuđih pristupnih podataka strogo je zabranjena i predstavlja grubo kršenje ove procedure.

17. Korisnik je dužan čuvati tajnost zaporke i ne otkrivati je drugim osobama, kako bi se spriječila zlouporaba njegovog korisničkog imena. Ukoliko korisnik posumnja da je

njegova zaporka kompromitirana, treba hitno obavijestiti urednika ili tehničkog urednika mreže i intraneta.

18. U posebnim slučajevima, kad postoji opravdana sumnja u kršenje odredbi ove procedure, radi zaštite sustava i po zahtjevu ovlaštenih državnih ustanova, Veleučilište može dopustiti pregledavanje i nadzor sadržaja koje pojedini korisnik objavljuje. Sadržaj sustava može biti pod nadzorom radi podrške operativnim, korektivnim, sigurnosnim i istražnim akcijama.

19. U skladu s općeprihvaćenom poslovnom praksom, uredništvo weba prikuplja statističke podatke o uporabi sustava. Statistički podaci mogu obuhvatiti korisnička imena, veličine i nazive objavljenih dokumenata i dokumenata u pripremi za objavu, datum i vrijeme objava i izvršenih izmjena, te ostale podatke. Uporaba i analiza tih podataka omogućuje održavanje i koordinaciju razvoja sustava.

KONTAKT

20. Pitanja u vezi s ovom procedurom mogu se uputiti uredništvu.

IS- 5
PROCEDURA ZA UPORABU POSLOVNIH SUSTAVA

DEFINICIJE

1. Poslovne sustave objedinjavaju poslužitelji s odgovarajućim operacijskim sustavima, bazama podataka koje sadrže poslovne podatke, aplikacijske i klijentske postavke, te klijentske aplikacije na klijentskim računalima. Klijentskim aplikacijama odvijaju se kontrolirana ažuriranja, pretraživanja i dobavljanja podataka iz baza, te se upravlja pravima pristupa i mogućnostima korisnika na razini aplikacija.

ADMINISTRATORSKE RAZINE POSLOVNIH SUSTAVA

2. Administrator sustava i baze podataka. Administrator sustava - prva razina kojom se administrira cjelokupni operacijski sustav poslužitelja (upravlja radom, raspodjelom i korištenjem računalnih resursa, upravlja ovlastima i pravima korisničkih računa, upravlja datotekama i aplikacijama na poslužitelju). Ovaj korisnik nema pristup pojedinačnim zapisima poslovne baze, odnosno, ne može vidjeti podatke i njihov sadržaj - vidi bazu podataka kao cjelinu (kao skup datoteka).

3. Administrator baze podataka - druga razina kojom se administrira pristup bazi podataka upravlja pravima pristupa bazi podataka, održava i nadograđuje sustav baze, ima pristup do svih resursa i njima može neograničeno upravljati.

4. Administrator aplikacije - treća razina kojom se administrira pristup pojedinim modulima aplikacije, određuju prava njihova korištenja.

5. U izuzetnim slučajevima, a po odobrenju Menadžera IT sigurnosti, administratori iz točaka 2, 3 i 4 mogu biti ista osoba.

ADMINISTRIRANJE KORISNIKA POSLOVNIH SUSTAVA

6. Administrator aplikacije obavlja sve poslove ažuriranja prava i ovlasti svih korisnika unutar poslovnih sustava.

7. Preduvjet korisnikova pristupa poslovnim sustavima je da korisnik ima aktivan korisnički račun unutar informacijskog sustava Veleučilišta.

8. Korisnički račun unutar informacijskog sustava Veleučilišta otvara se na temelju članka 10. Pravilnika o računalnoj informacijskoj sigurnosti. Zahtjev se dostavlja vidu popisa za više korisnika odjednom ili pojedinačno na obrascu *„Zahtjev za administraciju korisnika“,* a koji treba obavezno sadržavati:
   - ime i prezime osobe kojoj se otvara korisnički račun,
   - OIB za zaposlenike, odnosno JMBAG za studente,
   - adresa e-pošte,
   - naziv ustrojbene cjeline za zaposlenike, odnosno naziv studija za studente,
   - za zaposlenike naziv radnog mjesta,
   - datum dostavljanja zahtjeva.

9. Administrator je dužan je u najkraćem mogućem roku zaposleniku otvoriti korisnički račun, te ga uputiti na način prijavljivanja i odjavljivanja u informacijski sustav Veleučilišta, odnosno u pojedini poslovni sustav.

10. Korisnik poslovnog sustava dužan je čuvati tajnost podataka. Prije početka rada potrebno ga je upoznati s njegovim pravima i obavezama te zatražiti potpis na izjavu o čuvanju tajnosti podataka. Izjava se potpisuje u dva primjerka od kojih jedan ostaje korisniku, a drugi se čuva u sefu Odsjeka za informatičku potporu ili u Odjelu za marketing i kadrovske poslove.

11. Ostale postupke ažuriranja korisnika i njihovih prava i uloga unutar poslovnih sustava administrator aplikacije vrši samostalno u skladu sa svojim ovlaštenjima i odgovornostima, kao i po nalozima ovlaštenih osoba.

PODRŠKA KORISNICIMA POSLOVNIH SUSTAVA

12. U slučaju potrebe za podrškom i pomoći korisnik zove administratora aplikacije i opisuje svoje potrebe i/ili poteškoće. a slučaju da mu je administrator aplikacije nedostupan zove voditelja Odsjeka za informatičku potporu

1. Administrator aplikacije na temelju korisnikovog opisa nastoji otkriti stanje i uzrok korisnikove poteškoće, te ga uputiti kako je najbolje riješiti, ako je to u domeni znanja, ovlasti i sposobnosti administratora aplikacije. Ako korisnikove potrebe i problem nadilaze mogućnost rješavanja na ovoj razini administrator aplikacije zove voditelja Odsjeka za informatičku potporu ili njegovog zamjenika.

13. Voditelj Odsjeka za informatičku potporu, odnosno njegov zamjenik na temelju poziva iz točke administratora aplikacije ili korisnika, nastoji otkriti stanje i uzrok te uputiti korisnika na način rješavanja problema. Voditelj ili njegov zamjenik mogu delegirati zadatak za rješavanjem nastalih potreba ili problema svojim djelatnicima ukoliko je rješenje u domeni njihovog znanja, ovlasti i sposobnosti.

14. Ako pak korisnikove potreba i/ili problem nadilaze mogućnosti rješavanja na razini Odsjeka za informatičku potporu voditelj Odsjeka za informatičku potporu, a u skladu s ugovornim obvezama traži pomoć od vanjskog ugovornog partnera zaduženog za podršku poslovnom sustavu.

ODRŽAVANJA POSLOVNIH SUSTAVA OD STRANE VANJSKIH UGOVORNIH SURADNIKA

15. Sustavu može pristupiti i fizička osoba koja nije zaposlenik Veleučilišta, temeljem ugovora o korištenju i/ili održavanju poslovnog sustava ili pisanog naloga Dekana.

16. Prilikom svakog pristupa stranih osoba, koje nisu zaposlenici Veleučilišta poslovnim sustavima:
    - Voditelj Odsjeka za informatičku potporu, odnosno njegov zamjenik dužni su osigurati potrebna fizička i privremena korisnička prava pristupa osobama uz provjeru identiteta.
    - Odsjek za informatičku potporu evidentira osobe iz točke 15. u posebno određenu knjigu evidencije pristupa poslovnim sustavima (*Log Book*) prije samog neposrednog pristupa poslovnom sustavu

17. Evidencija pristupa poslovnim sustavim osoba iz točke 15. mora sadržavati podatke:
    - datum,
    - ime i prezime,
    - naziv tvrtke koju predstavljaju ili tekst "Po nalogu Dekana" ukoliko poslovnim sustavima pristupaju,
    - razlog pristupa i planirane aktivnosti,
    - očekivani rezultat pristupa i planiranih aktivnosti, te
    - vrijeme završetka pristupa,
    - koje su planirane aktivnosti izvršene,
    - koje su dodatne aktivnosti izvršene,
    - rezultat pristupa i izvršenih aktivnosti, te

- eventualne opaske.

18. Po završenom pristupu poslovnim sustavima i upisu podataka iz točaka 15. - 17. voditelj Odsjeka za informatičku potporu, odnosno njegov zamjenik, dovode sustav u stanje uobičajene sigurnosti i uskraćuju daljnje pravo pristupa osobama iz točke 15.

IS- 6
PROCEDURA ZA UPRAVLJANJE POVJERLJIVIM I VAŽNIM PODACIMA

KLASIFIKACIJA INFORMACIJA

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

Prema stupnju tajnosti, informacije mogu biti povjerljive, tajne ili vrlo tajne.

Kategorije službene, državne i vojne tajne pripadaju tijelima državne uprave.

Poslovna tajna su informacije koje imaju komercijalnu vrijednost i čije bi otkrivanje moglo nanijeti štetne posljedice Ustanovi ili njenim poslovnim partnerima (ugovori, financijski izvještaji, planovi, rezultati istraživanja itd.)

Profesionalna tajna odnosi na zanimanja poput liječnika, svećenika i odvjetnika, no može se primijeniti i na zaposlene koji u svom radu dolaze u dodir s podacima 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 podacima koji pripadaju korisnicima računala.

Dokumenti koji izvana dolaze u Ustanovu s nekom od oznaka povjerljivosti određuju stupanj povjerljivosti svih dokumenata i informacija koje će Ustanova 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.

RASPODJELA ODGOVORNOSTI

Za klasificiranje povjerljivih informacija zadužen je u rukovoditelj Ustanove, koji će izraditi listu osoba koje imaju pravo proglasiti podatke tajnima, te listu osoba koje imaju pristup povjerljivim podacima.

Pravila za čuvanje povjerljivih informacija odnose se na sve zaposlenike Ustanove i vanjske suradnike koji dolaze u doticaj sa osjetljivim podacima. Obaveza čuvanja povjerljivosti ne prestaje s prestankom radnog odnosa.

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 liste zaposlenika koji imaju ovlasti, te bilježenjem vremena izdavanja i vraćanja dokumenata, kako bi se u svakom trenutku znalo gdje se oni nalaze.

INFORMACIJE O ZAPOSLENICIMA

Socijalni inženjering je metoda koju primjenjuju hackeri kako bi prikupili informacije potrebne za provalu na računala.

Ustanova može informacije o zaposlenima koje se smatraju javnima objaviti na svojim web stranicama. Javnim informacijama smatraju se:

- ime i prezime
- posao koji zaposlenik obavlja
- broj telefona na poslu
- službena e-mail adresa

Na upite o zaposlenicima davati će se samo informacije objavljene na internim web stranicama. Daljnje informacije o zaposlenima ne smiju se davati bez suglasnosti osobe kojoj

podaci pripadaju (na pr. adresa stana, broj privatnog telefona, podaci o primanjima, porezu, osiguranju itd.)

Povjerljive informacije u načelu se ne daju se telefonom jer se sugovornik može lažno predstaviti. Ukoliko se sugovornik predstavlja kao službena osoba koja ima pravo pristupa povjerljivim podacima, zapisuje se ime i prezime te osobe, naziv institucije kojoj pripada i broj telefona s kojeg zove. Nakon provjere istinitosti tih podataka zaposlenik Ustanove će se posavjetovati s upravom i ukoliko dobije odobrenje nazvati službenu osobu i odgovoriti na pitanja.

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.

Ako se povjerljive informacije šalju elektronički, na primjer kao poruke elektroničke pošte, tada se moraju slati kriptirane.

KOPIRANJE POVJERLJIVIH INFORMACIJA

Za kopiranje povjerljivih informacija treba zatražiti dozvolu vlasnika informacije.

Povjerljivi dokumenti koji izvana dođu u Ustanovu ne smiju se kopirati bez izričite dozvole pošiljatelja.

Dokumenti koji pripadaju Ustanovi 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 obavezati da odbiju kopiranje povjerljivih dokumenata ukoliko nije ispoštovana propisana procedura.

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, obavezno je uništavanje podataka sa diskova posebnim programom koji nepovratno prebriše sadržaj diska.

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 premjestiti na drugo radno mjesto na kojem neće dolaziti u dodir s povjerljivim podacima.

S vanjskim suradnicima za koje se ustanovi da otkrivaju povjerljive informacije razvrgnuti će se ugovor. Stoga ustanova treba već u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.

IS- 8
PROCEDURA ZA ANTIVIRUSNU ZAŠTITU I ZAŠTITU OD SPAMA

Virusi i crvi predstavljaju opasnost za informacijske sustave, ugrožavajući funkcioniranje mreže i povjerljivost podataka.

Nove generacije virusa su izuzetno složene i opasne, sposobne da prikriju svoje prisustvo, presreću unos podataka na tipkovnici. Informacije poput zaporki ili povjerljivih dokumenata mogu slati svome tvorcu nekamo na Internet, te otvoriti kriptiran kanal do vašeg računala, kako bi hackeri preuzeli kontrolu nad njim.

Stoga zaštita od virusa ne smije više biti stvar osobnog izbora, već obaveza ustanove, administratora računala i svakog korisnika.

Ustanova propisuje da je zaštita od virusa obavezna i da se provodi na nekoliko razina:

- 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 sa 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.

NEPRIDRŽAVANJE

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

SVRHA

Internetom putuje sve više neželjenih komercijalnih poruka, tzv. spam. Masovne poruke elektroničke pošte najjeftiniji su način reklamiranja. Cijenu plaćaju korisnici i tvrtke, jer čitanje i brisanje neželjenih poruka troši radno vrijeme i umanjuje produktivnost.

Dio neželjenih poruka nastoji uvući primatelja u kriminalne aktivnosti, na primjer otvaranje računa za pranje novca, ili su prijevara, nastoje pobuditi samilost kako bi se izvukao novac (enlg. hoax). Za prepoznavanje ovakvih poruka korisnici mogu koristiti uslugu CARNet CERT-a Hoax recognizer.

PRAVILA ZA ADMINISTRATORE

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

Prva mogućnost jest da se definira 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 neće se primati.

Druga razina zaštite je automatska provjera sadržaja. Poslužitelj može poruke koje su obilježene kao spam spremati na određeno vrijeme u karantenu.

Treću razinu zaštite određuju sami korisnici. Poruke dobijaju bodove koji ukazuju na vjerojatnost da se radi o spamu. Kako nije uvijek moguće pouzdano definirati što je spam, ovakva zaštita mora biti uvjetna, odnosno krajnjem korisniku se prepušta uključivanje bodovanja i konfiguriranje preusmjeravanja označenih poruka.

Informatičar zadužen za sigurnost će obučiti korisnike i pomagati im pri kreiranju filtera za obilježavanje, odvajanje ili uništavanje neželjenih poruka.

PRAVILA ZA KORISNIKE

Korisnici ne smiju slati masovne poruke, bez obzira na njihov sadržaj. Upozorenja na viruse su često lažna i šire zablude. Korisnici ne smiju radi stjecanja dobiti odašiljati propagandne poruke koristeći računalnu opremu koja pripada ustanovi.

NEPRIDRŽAVANJE

Protiv korisnika koji se oglušuju o pravila prihvatljivog korištenja i šalju masovne neželjene poruke biti će pokrenut stegovni postupak.

IS- 9
PROCEDURA ZA RUKOVANJE ZAPORKAMA

Zaporke su najčešće upotrebljavan mehanizam autentifikacije korisnika. Međutim, zbog neprimjerenih navika korisnika informacijskog sustava (primjerice dijeljenja zaporka i njihove neadekvatne pohrane te upotrebe neprimjerenih zaporka) one su i jedan od najslabijih mehanizama autentifikacije. Primjereno upravljanje zaporkama (koje uključuje uklanjanje poznatih ranjivosti i prevenciju uobičajenih napada) može uvelike unaprijediti sigurnost informacijskog sustava.

Napadi na zaporke odnosno pokušaji njihova otkrivanja ili zaobilaženja jedna su od najčešćih vrsta napada na informacijske sustave. Neke od najčešćih podvrsta napada na zaporke jesu:

- pokušaj pogađanja zaporka isprobavanjem svih kombinacija dopuštenih simbola (engl. dictionary attack)
- pokušaj pogađanja zaporka pomoću specifičnih informacija o osobi koja rabi tu zaporku (primjerice ime supružnika, imena djece, ime kućnog ljubimca i slično)
- pokušaj neautorizirane autentifikacije pomoću standardnih zaporka koje inicijalno definiraju proizvođači hardvera, softvera i telekomunikacijske opreme
- pokušaj neautorizirane autentifikacije pomoću zaporka čija je povjerljivost narušena zbog neadekvatne pohrane.

Zbog mnogobrojnih ranjivosti koje proizlaze iz neadekvatnog korištenja zaporki, te velikog broja prijetnja koje pokušavaju iskoristiti te ranjivosti, banka bi trebala propisati restriktivne postupke upravljanja zaporkama, kako bi se osjetljivost na tu vrstu napada svela na najmanju moguću mjeru.

Pri upravljanju zaporkama odsjek za informatičku podršku bi trebao uzeti u obzir barem sljedeće:

1. Minimalna dužina zaporke

Kratku zaporku lakše je probiti. Stoga neka minimalna dužina zaporke bude šest znakova, ali preporučujemo korištenje još dužih zaporki.

2. Ne koristiti riječi iz rječnika

Hackeri posjeduju zbirke rječnika, što im olakšava probijanje ovakvih zaporki (tzv. dictionary attack).

3. Izmiješati mala i velika slova s brojevima

Na primjer: h0bo3niCa. Na prvi pogled besmislena i teška za pamćenje, ova je zaporka izvedena iz riječi hobotnica. Polazište je pojam koji lako pamtimo, ali onda po nekom algoritmu vršimo zamjenu znakova.

4. Ne koristiti imena bliskih osoba, ljubimaca, datume

Takve se zaporke lako otkriju socijalnim inženjeringom.

5. Trajanje zaporke

Promjena zaporke smanjuje vjerojatnost njezina otkrivanja. Neki korisnici naizmjence koriste dvije standardne zaporke. Iako su dvije zaporke bolje nego jedna, ipak se ovakvim trikovima izigrava osnovna svrha promjene zaporki.

6. Tajnost zaporke

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

Hakeri nastoje izmamiti zaporke lažno se predstavljajući kao administratori. Pravi administratori imaju mogućnost rješavanja probleme i bez poznavanja korisničkih zaporki.

7. Čuvanje zaporke

Zaporke se ne ostavljaju na papirićima koji su zalijepljeni na ekran ili ostavljeni na stolovima, u nezaključanim ladicama itd. 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.

8. 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 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 da li su korisničke zaporke u skladu s navedenim pravilima.

IS-10
PROCEDURA ZA UPORABU PROSTORIJA PODATKOVNOG CENTRA

SVRHA DONOŠENJA

Osiguranje ispravnog funkcioniranja sobe s poslužiteljima računalnog informacijskog sustava Veleučilišta Velika Gorica, kao kritičnog dijela računalnog sustava, uvođenjem osnovnih pravila ponašanja, pristupa te kontrole.

OPĆENITO

Soba s poslužiteljima računalnog informacijskog sustava Veleučilišta Velika Gorica sastoji se od dviju prostorija. Jedna prostorija je radni prostor administratora sustava, dok je u drugoj smještena komunikacijska i poslužiteljska informatička oprema. U svaku od ovih prostorija ulazi se kroz zasebni ulaz, a u sobu s poslužiteljima može se ući i iz radne prostorije administratora sustava.

KONTROLA PRISTUPA

Odgovorna osoba za sobu s poslužiteljima je administrator sustava.

Vrata obaju prostorija moraju biti zaključana ako nije prisutan administrator sustava ili neki drugi . Prostorija s poslužiteljima uvijek mora biti zaključana.

Ključevi sobe s poslužiteljima koriste se jedino u slučaju potrebe, odnosno u slučaju kada za to postoji realna potreba koja se mora navesti u knjizi ulaska/izlaska iz sobe s poslužiteljima.

Najstrože je zabranjeno držanje ključa u bravi predprostora i sobe s poslužiteljima, ili na drugom neosiguranom mjestu.

U slučaju odsutnosti administratora sustava menadžer IT sigurnosti određuje zaposlenika Odsjeka za informatičku podršku koji preuzima odgovornost za korištenje sobe s poslužiteljima. O odluci o imenovanju zaposlenika odsjeka za informatičku podršku

odgovornog za postupanje po ovoj proceduri menadžer za IT sigurnost pismeno obavještava voditelja Službe za tehničke i opće poslove, te domara.?

Pričuvni ključevi sobe s poslužiteljima nalaze se: u zatvorenoj i zapečaćenoj koverti u prostorija domara i čistaćica – skladište u prizemlju glavne zgrade u zaključanom ormariću ili u drugom osiguranom prostoru

U slučaju potrebe korištenja poslužiteljske sobe od strane djelatnika Veleučilišta koji su ovlašteni od strane menadžera za IT sigurnost, potrebno je najaviti voditelju odsjeka za informatičku podršku ili menadžeru za sigurnost te navesti podatke u knjizi ulaska/izlaska iz sobe s poslužiteljima.

Postupak ovlaštenja djelatnika Veleučilišta Velika Gorica za pristup predprostoru i prostoru s poslužiteljima se vodi u knjizi ovlaštenja.

U interventnim situacijama na isti način ključ može preuzeti i djelatnik Pododsjeka za ugostiteljstvo i uslužne djelatnosti Veleučilišta Velika Gorica. Pritom je prije ulaska dužan obavijestiti odgovorne osobe i napisati zapisnik i izvješće o potrebi izvanrednog ulaska u sobu s poslužiteljima, koje elektroničkim putem dostavlja administratoru sustava i voditelju Službe tehničkih i općih poslova.

Pravo pristupa imaju sljedeće osobe:

1. Samostalan ulaz bez najave uz evidentiranje u knjizi ulaska/izlaska iz sobe s poslužiteljima koja se nalazi u radnoj prostoriji administratora sustava:

    a. voditelj Informatičkog centra,

    b. administrator sustava.

2. Samostalan ulaz s najavom voditelju odsjeka za informatičku podršku, menadžeru za IT sigurnost ili administratoru sustava i upisom u evidenciju u knjigu ulaska/izlaska iz sobe s poslužiteljima koja se nalazi na vratima sobe s poslužiteljima :

    a. zaposlenici Informatičkog centra

    b. ovlaštene osobe od strane menadžera za IT sigurnost

3. Osobe koje ulaze samo u pratnji osoba navedenih pod točkom 1.:

    a. Mogućnost ulaska u sobu s poslužiteljima računalnog informacijskog sustava Veleučilišta Velika Gorica imaju i članovi Uprave Veleučilišta, ali isključivo u pratnji odgovorne osobe iz grupe 1.

4. Pristup vanjskih suradnika, partnera, servisera sobi s poslužiteljima:

a. Vanjski suradnici obvezno se evidentiraju u knjigu ulazaka/izlazaka stranaka

b. Prilikom ulaska u sobu s poslužiteljima obvezno moraju biti u pratnji osoba iz točke 1.

c. Sve radove moraju nadgledati osobe iz točke 1, te o učinjenom, elektroničkim putem izvijestiti voditelja Informatičkog centra.

PREVENTIVNO ODRŽAVANJE

1. Preventivno održavanje poslužitelja moguće je obaviti unutar sobe s poslužiteljima ili izvan nje što ovisi o mogućnostima njihove dislokacije, no poželjnije je van nje kako bi se smanjilo vrijeme zadržavanja u njoj.

UREDNOST

1. Soba s poslužiteljima mora biti uredna i bez nepotrebnih stvari (u njoj smije biti isključivo oprema) što znači da je treba konstantno održavati čistom, za što su nadležne odgovorne osobe.

2. Obvezno je redovno spremanje i čišćenje sobe s poslužiteljima: poda, prozora, povremeno ispuhivanje prašine sa sadržaja ormara), te izbacivanje nepotrebnih stvari (kabeli, šine, alat i sl. ne smiju se odlagati u serverskoj sobi).

3. Zabranjeno je unošenje hrane i pića u sobu s poslužiteljima.

4. Zabranjeno je pušenje u sobi s poslužiteljima.

5. Zabranjeno je svako nepotrebno zadržavanje u sobi s poslužiteljima, osim za gore navedene poslove.

IZVANREDNE SITUACIJE

1. U slučaju izvanredne situacije (požar) potrebno je pristupiti manualnoj aktivaciji protupožarnog sustava (PP aparati, unutarnja hidrantska mreža) od strane zaštitara ili radnika.

2. U slučaju kvara sustava, osobe ovlaštene za pristup sobi s poslužiteljima dolaze na lokaciju (ukoliko nije moguće udaljeno otkloniti kvar) te pristupaju otklanjanju nastalog kvara.

PRILOZI PROCEDURI:

1. Zapisnik i izvješće o potrebi izvanrednog ulaska u sobu s poslužiteljima,
2. knjiga ulaska/izlaska iz sobe s poslužiteljima.
3. Knjiga ovlaštenja

PRILOZI PROCEDURI ZA UPORABU PROSTORIJA PODATKOVNOG CENTRA

PRILOG 1. Zapisnik i izvješće o potrebi izvanrednog ulaska u sobu s poslužiteljima

Rb.	DATUM OTVARANJA KOVERTE	IME I PREZIME OSOBE KOJA OTVARA KOVERTU	RAZLOG OTVARANJA KOVERTE	ODOBRIO OTVARANJE

PRILOG 2: Knjiga ulaska/izlaska iz sobe s poslužiteljima

RB.	DATUM	IME I PREZIME POSJETITELJA	OIB POSJETITELJA	POTPIS POSJETITELJA	RAZLOG POSJETE	NADZORNA OSOBA I POTPIS

PRILOG 3: Knjiga ovlaštenja

RB.	IME I PREZIME OVLAŠTENIKA	USTANOVA OVLAŠTENIKA	OVLASTIO

IS-11
PROCEDURA SIGURNOSNE POHRANE PODATAKA

Politike sigurnosnih kopija imaju namjeru da jednoznačno u cijeloj organizaciji definiraju načine postupanja prema podacima, načine izrade sigurnosnih kopija te vraćanja podataka u slučaju određenih gubitaka. Rizik koji se odnosi prema informacijama određuje svaki korisnik zasebno, a učestalost izvođenja izrade sigurnosnih kopija se određuje u skladu s važnošću informacija i pripadajućim rizikom. Postupak izrade sigurnosnih kopija i vraćanje podataka treba biti dokumentiran u obliku procedure i primjenjiv u svim dijelovima organizacije.

Što se tiče fizičkog smještaja medija potrebno je da se na isti primjenjuju što je moguće viši nivoi zaštite. Politika sigurnosnih kopija nalaže da se u određenim vremenskim periodima provjeri i testira vraćanje podataka s medija. Mediji trebaju biti na odgovarajući način označeni što podrazumijeva da sadrže sistemsko ime, datum stvaranja, klasifikaciju važnosti podataka i kontaktne informacije. Ukoliko se ne pridržava navedenih procedura politika propisuje i odgovarajuće disciplinske akcije.

Ova procedura propisuje sljedeće stavke:

• svi podaci se tretiraju kao povjerljivi i tajni od strane korisnika i činjenica da su snimljeni u elektroničkom obliku ne sprječava da se prema njima ne odnosi kao prema povjerljivim i tajnim,

• podaci su vlasništvo organizacije i ukoliko korisnik napušta istu potrebno je organizaciji prepustiti sva prava na podatke,

• dio organizacije koji ima vlasništvo na proces izrade sigurnosnih kopija mora poduzeti odgovarajuće korake kako bi se osigurao integritet podataka i sigurnost svih aplikacija i podataka generiranih njima,

• nadležna služba, odnosno odsjek za informatičku podršku mora omogućiti adekvatnu kontrolu pristupa podacima na sigurnosnim kopijama i nadgledati sustav u smislu ispravnog korištenja. Pristup mora biti prikladno dokumentiran, autoriziran i kontroliran,

• svi odjeli unutar organizacije moraju imaju planove kontinuiranog odvijanja poslovanja u skladu s pripadajućim rizicima i poslovnih zahtjevima (ovo podrazumijeva redovito testiranje vraćanja podataka),

• svi ugovori, licence i slično trebaju imati odgovarajuće sigurnosne kopije s ciljem povećanja opće sigurnosti sustava organizacije,

• svi sustavi koji se nalaze izvan organizacije moraju biti nadgledati od strane organizacije i a njih se primjenjuju politike sigurnosnih kopija kao i u samoj organizaciji

Dobra praksa sigurnosne pohrane je svakodnevno, tjedno i mjesečno pohranjivanje informacijskih sustava (Pretinac, gaudeamus, synesis, nyon) i podataka korisnika na lokaciji unutar Veleučilišta Velika Gorica te na izdvojenim lokacijama, a to su:

- CARnet
- vanjska ustanova (Magis informatics d.o.o) koja je ugovorno održavatelj računalnog sustava Veleučilišta Velika Gorica

Sigurnosnu pohranu podataka izvršava odsjek za informatičku podršku Veleučilišta.

PRILOG PROCEDURI:

1. Pohrana - Backup

PRILOG PROCEDURI „SIGURNOSNE POHRANE PODATAKA“ – POHRANA – BACKUP

Pohrana – BACKUP

SADRŽAJ KOJI JE POHRANJEN: _____

DATUM POHRANE: _____

IME, PREZIME, TELEFON, ADRESA OSOBE KOJA JE POHRANILA PODATKE:

_____

PROGRAMSKI „ALAT“ POMOĆU KOJEG JE UZETA KOPIJA: _____

LOKACIJA POHRANE: _____

DATUM POSLJEDNJE KONTROLE O ISPRAVNOSTI POHRANJENIH PODATAKA:

_____

IME PREZIME OSOBE KOJA JE IZVRŠILA PRETHODNU KONTROLU:

_____