Temeljem članka 24. Zakona o informacijskoj sigurnosti (NN 79/03), Stručno vijeće Sveučilišnog odjela za stručne studije, na 19. sjednici održanoj dana 21. svibnja 2014. g. donijelo je

PRAVILNIK O SIGURNOSTI INFORMACIJSKIH SUSTAVA

Uvodne odredbe

Članak 1.

Ovim se pravilnikom uređuje sigurnost upravljanja informacijskim sustavima na Sveučilišnom odjelu za stručne studije u Splitu (u nastavku Odjel), definiraju prihvatljivi načini ponašanja i jasna raspodijela uloga i odgovornosti svih čimbenika informacijskog sustava.
Novi zaposlenici dužni su se upoznati s njegovim odredbama prilikom zapošljavanja, a studenti prilikom otvaranja korisničkih računa.
Pravila rada i ponašanja koja su definirana sigurnosnom politikom odnose se na:

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

Članak 2.

U ovom Pravilniku koriste se pojmovi sa sljedećim značajem:

- davatelji usluga - djelatnici Službe za informacijske tehnologije Odjela (u nastavku IT služba), ovlašteni CARNet sistem inženjeri te stručni suradnici za informacijske sustave ovlašteni od strane Službe za informacijske tehnologije ili Pročelnika Odjela.
- korisnici informatičkih usluga - osobe koje se u svom radu ili učenju služe računalima, proizvode dokumente ili unose podatke, ali ne odgovaraju za instalaciju i konfiguraciju softvera, niti za ispravan i neprekidan rad računala i mreže. Korisnici informacijskog sustava su svi zaposlenici Odjela, vanjski suradnici i studenti.
- glavni korisnik – osoba odgovorna za rad pojedine aplikacije u okviru informacijskog sustava, a koja je od vitalne važnosti za Odjel ili neki njegov dio.
- koordinator za informiranje - osoba odgovorna za pravovremeno i redovito ažuriranje svih informacija koje se postavljaju na javne servise za informiranje.
- specijalisti za sigurnost - osobe i tijela koja se brinu o organizaciji i provođenju sigurnosnih mjera definiranih ovim Pravilnikom.
- ekipa za hitne intervencije - djelatnici Službe za informacijske tehnologije i CARNet sistem inženjer poslužitelja kojeg je za to ovlastio Voditelj IT službe.
- povjerenstvo za sigurnost - tijelo koje upravlja sigurnošću informacijskog sustava Odjela

- zona javnih servisa - oprema koja obavlja javne servise Odjela. U ovu opremu svrstavaju se: DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte, FTP poslužitelj itd.).
- intranet - privatna mreža Odjela koju sačinjavaju poslužitelji internih servisa, osobna računala zaposlenih, računalne učionice te komunikacijska oprema lokalne mreže. Računala iz ove grupe dijele se na: studentska računala, računala administrativnog osoblja, računala akademskog i nastavnog osoblja, poslužiteljska računala, sigurnosne uređaje i nastavna računala.
- extranet - proširenje privatne mreže otvoreno mobilnim korisnicima, poslovnim partnerima ili veza između izdvojenih lokacija, zasebnih intraneta. U ovu grupu spadaju veze lokalnih baza podataka s središnjim poslužiteljima (LDAP, ISVU, X-ice, baze knjižnice) i sl.
- prijenosna računalna oprema - sastoji se od prijenosnih računala u vlasništvu Odjela koja zaposlenici koriste izvan prostora Odjela i u prostoru Odjela. Takvu računalnu opremu zaposlenici Odjela smiju priključivati na fiksnu lokalnu mrežu samo na za to predviđenim mjestima i uz prethodnu suglasnost IT službe Odjela.

Organizacija upravljanja sigurnošću

Članak 3.

Osobe koji se u radu koriste računalima dijele se na davatelje i korisnike informatičkih usluga.

Davatelji informatičkih usluga odgovaraju za ispravnost i neprekidnost rada informacijskog sustava. Samo davatelji smiju biti administratori računala koja se koriste na Odjelu.

IT služba Odjela može iznimno, na opravdani zahtjev korisnika ili uprave Odjela, odrediti administratora računala koji nije iz grupe davatelja informatičkih usluga. U tom slučaju ta je osoba dužna pismeno potvrditi potpunu odgovornost za opremu i softver koji administrira te odgovornost za sve posljedice koje iz toga proizlaze. To potvrđuje potpisom Izjave o administriranju računala.

Korisnici informatičkih usluga dužni su:

- pridržavati se pravila prihvatljivog korištenja, to jest da ne koriste računala za radnje koje nisu u skladu sa važećim zakonima, etičkim i moralnim normama, Etičkim kodeksom Odjela i Pravilnikom o sigurnosti informacijskih sustava Sveučilišnog odjela za stručne studije u Splitu,
- prijaviti svaki sigurnosni incident,
- izabrati kvalitetnu zaporku i povremeno je mijenjati,
- ukoliko korisnici u svom radu proizvode podatke i dokumente, odgovorni su za vjerodostojnost tih podataka, te za njihovo čuvanje kao i za izradu sigurnosnih kopija podataka.

Članak 4.

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

Članak 5.

Svaka aplikacija koju Odjel koristi za obradu podataka, a koja je od vitalne važnosti za Odjel ili jedan njegov dio, mora imati glavnog korisnika.

Glavnog korisnika aplikacije određuje uprava Odjela na temelju specifičnosti pojedine aplikacije i odgovornosti zaposlenika, a na prijedlog IT službe Odjela.
Glavni korisnik je u pravilu voditelj određene službe, odsjeka, zavoda ili nositelj nekog projekta.

Zaposlenici kojima je glavni korisnik nadređen unose podatke i odgovaraju za vjerodostojnost tih podataka.

Glavni korisnik odgovaran je za provjeru ispravnosti podataka, za provjeru ispravnosti aplikacije, te za sprečavanje neovlaštenog pristupa podacima i za sprečavanje izmjene podataka od strane neautoriziranih osoba.

Podatke o glavnim korisnicima pojedine vitalne aplikacije dužna je voditi IT služba Odjela.

Prihvatljivo korištenje računalne i mrežne opreme

Članak 6.

Računalna i mrežna oprema Odjela, CARNet mreža i sve dostupne usluge na raspolaganju su korisnicima radi obavljanja posla, odnosno za učenje, poučavanje i istraživanje. Ova prava korisnici su dužni ostvarivati poštujući potrebe i prava ostalih korisnika. Od svih ustanova spojenih na CARNet mrežu, kao i od njihovih korisnika, očekuje se odgovornost pri korištenju informacijskih resursa. Prihvatljivo korištenje računalne mreže Odjela te CARNet mreže je svako korištenje u skladu s ovim pravilima.

Neprihvatljivo korištenje računalne i mrežne opreme

Članak 7.

Neprihvatljivim korištenjem se smatra svako korištenje računala i računalne mreže na način koji bi doveo do povrede zakona, propisa ili etičkih normi, a mogao bi izazvati materijalnu ili nematerijalnu štetu za Odjel, CARNet, ostale ustanove članice CARNet mreže i bilo koje treće osobe.

Članak 8.

Nije dopušteno korištenje, stvaranje ili prijenos mrežom, osim eventualno u okviru znanstvenog istraživanja:

- materijala koji je napravljen da bi izazvao neugodnosti, neprilike ili širio strahove
- uvredljivog i ponižavajućeg materijala,
- materijala koji su zaštićeni autorskim pravima, bez dozvole vlasnika prava ili plaćanja naknade,
- korištenje računalne mreže Odjela i CARNet mreže na način koji ometa druge korisnike u njezinom korištenju, poput preopterećivanja pristupnih linija, mrežne opreme i poslužitelja,
- širenje virusa i ostalih malicioznih programa,
- slanje neželjenih masovnih elektroničkih poruka ,
- upotreba računalnih resursa izvan granica ili na načina koji je korisniku odobren. Ukoliko nije siguran glede prava i načina upotrebe neke usluge, korisnik je dužan obratiti se IT službi Odjela.

Također nije dopušteno :

- preuzimanje tuđeg identiteta (primjerice, korištenje računala ili usluga pod tuđim imenom, slanje elektroničke pošte pod tuđim imenom, kupovanje preko interneta tuđom kreditnom karticom i slično),
- provaljivanje na bilo koja računala i preuzimanje njihove kontrole,
- traženje sigurnosnih propusta na bilo kojoj računalnoj opremi bez dozvole vlasnika opreme,
- izvršavanje napada uskraćivanjem resursa (eng. Denial of Service),
- korumpiranje ili uništavanje podataka ostalih korisnika,
- povreda privatnosti ostalih korisnika.

Članak 9.

Računalnu opremu nije dopušteno ostavljati bez nadzora ukoliko nije adekvatno zaštićena od neovlaštenog pristupa i korištenja.

Članak 10.

Računala koja nisu vlasništvo Odjela mogu se priključiti na računalnu mrežu Odjela isključivo uz odobrenje IT službe Odjela. U tom slučaju ti se korisnici moraju pridržavati svih pravila iz ovog dokumenta, a njihova računala moraju udovoljavati svim pravilima.

Članak 11.

Odjel u potpunosti prihvaća CARNetov dokument CDA 0035 - Odluka o prihvatljivom korištenju CARNet mreže koji je dostupan na adresi

ftp://ftp.carnet.hr/pub/CARNet/docs/info/CDA0035-2.pdf

Članak 12.

Specijaliste za sigurnost predstavljaju: Ekipa za hitne intervencije i Povjerenstvo za sigurnost.

Sigurnosne mjere provode se na dojavu o sigurnosnom incidentu od strane CARNet-a ili vlastitim utvrđivanjem incidenta koji je nastao kao produkt neprihvatljivog korištenja računalne opreme od strane korisnika Odjela.

Za fizičku sigurnost informacijskog sustava brine se IT služba. Ostali djelatnici zaduženi za fizičku sigurnost objekata (domari, portiri, čuvari i sl.) dužni su surađivati sa IT službom.

Članak 13.

Voditelj IT službe predlaže pravilnike, organizira nadzor rada mreže i servisa, sudjeluje u organizaciji obrazovanja korisnika i administratora, komunicira s upravom, sudjeluje u donošenju odluka o nabavi računala i softvera, te sudjeluje u razvoju softvera, kako bi se osiguralo poštivanje pravila iz ovog Pravilnika.

Članak 14.

Ekipa za hitne intervencije, po nalogu Voditelja IT službe poduzima radnje uz pomoć kojih otklanja posljedice incidenta na najbrži mogući način.

Po otklanjanju incidenta Ekipa za hitne intervencije izvještava Voditelja IT službe koji, ovisno o težini incidenta, odlučuje o daljnjim mjerama.

U slučaju težeg incidenta Voditelj IT službe sačinjava izvješće o sigurnosnoj situaciji koje predaje Povjerenstvu za sigurnost.

Članak 15.

Povjerenstvo za sigurnost sastavljeno je od Pročelnika Odjela, CARNet koordinatora, CARNet sistem inženjera, Voditelja IT službe, predstavnika studenata i predstavnika oštećenih korisnika ili korisnika osobno.

Povjerenstvo za sigurnost, na temelju izvješća o sigurnosnoj situaciji predlaže mjere za poboljšanje sigurnosti (nabava sigurnosne opreme i softvera, obrazovanje korisnika i specijalista...).

Povjerenstvo za sigurnost daje odobrenje za provođenje istrage u slučaju sigurnosnog incidenta i donosi odluke o mjerama za sankcioniranje odgovornih korisnika.

U slučaju sigurnosnog incidenta prouzrokovanog od strane osoba koje nisu korisnici Odjela, Povjerenstvo daje CARNet koordinatoru nalog za prijavu sigurnosnog incidenta CERT-u koji se nalazi u sastavu CARNet-a.

Administriranje računala

Članak 16.

IT služba Odjela dužna je administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.

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.

Članak 17.

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

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

Članak 18.

Administratori su dužni incidente prijaviti Voditelju IT službe, te pomoći pri istrazi i uklanjanju problema. Incidenti se dokumentiraju kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti. Ukoliko je incident ozbiljan i uključuje kršenje zakona, prijavljuje se CARNetovu CERT-u.

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

Članak 19.

Ukoliko napredni korisnici žele sami administrirati računalo kojim se služe, moraju predati pismeni zahtjev i potpisati Izjavu o administriranju računala, nakon čega za njih vrijede sva pravila za administriranje računala. U tom slučaju osobe su u potpunosti odgovorne za računalo, sav softver, podatke i dokumente na računalu te radnje koje se tim računalom obavljaju. IT služba na nijedan način nije odgovorna za takva računala.

Instalacija i licenciranje softvera

Članak 20.

Korištenje ilegalnog softvera predstavlja povredu autorskog prava i intelektualnog vlasništva. U dogovoru s korisnicima i ostalim stručnim službama, IT služba sudjeluje u nabavi te instalira i konfigurira softver isključivo uz uvjet da je on propisno licenciran.

Nadzor informacijskog sustava

Članak 21.

IT služba Odjela zadržava pravo nadzora nad cjelokupnom računalnom i mrežnom opremom u svom vlasništvu i u svojim prostorima, nad softverom i podacima koji se nalaze na toj računalnoj opremi te načinom korištenja opreme.

Članak 22.

Nadzor se smije provoditi radi:

- osiguranja integriteta, povjerljivosti i dostupnosti informacija
- provođenja istrage u slučaju sumnje u sigurnosni incident
- provjere da li je informacijski sustav i njegovo korištenje usklađeno s ovim pravilnikom

Članak 23.

Nadzor smiju obavljati samo osobe ovlaštene od strane Odjela. U pravilu su to djelatnici IT službe.
Pri provođenju nadzora ovlaštene osobe su dužne poštivati privatnost korisnika te povjerljivost podataka i informacija.
U slučaju kad korisnik prekrši pravila sigurnosne politike, povjerljivost informacija se više ne može osigurati i te se informacije mogu dalje koristiti u istrazi i daljnjim postupcima.

Članak 24.

Korisnici su dužni pomoći osobama zaduženim za nadzor informacijskih sustava i to na način da im pruže sve informacije i omoguće im pristup prostorijama i opremi radi provođenja nadzora.

Fizička sigurnost

Članak 25.

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

Ustanova je dužna sastaviti popis osoba koje imaju pravo pristupa u zaštićena područja, a porta mora imati popis osoba koje mogu dobiti ključeve određenih prostorija.

Članak 26.

Računalna i mrežna oprema koja obavlja kritične funkcije, neophodne za rad informacijskog sustava Odjela ili sadrži povjerljive informacije, fizički je odvojena u prostor u koji je ulaz dozvoljen isključivo ovlaštenim osobama, tzv. sigurna zona.

Ustanova je dužna napraviti popis ovlaštenih osoba koje imaju pristup sigurnim zonama. U pravilu su to djelatnici IT službe Odjela koji administriraju poslužitelje i mrežnu opremu.

Članak 27.

Povremeno se u sigurnim prostorima mora dopustiti pristup osobama iz vanjskih tvrtki ili ustanova, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja itd. Ustanova može u ugovore s vanjskim tvrtkama uvrstiti odredbe kojima obvezuje poslovne partnere na poštivanje sigurnosnih pravila. Ugovorom se regulira pristup prostorijama, pristup opremi i pristup povjerljivim podacima.

Članak 28.

U slučaju da u sigurnu zonu radi potrebe posla ulaze osobe koje nemaju ovlasti, mora im se osigurati pratnja od strane davatelja informatičkih usluga. Strana osoba može se ostaviti da obavi posao u zaštićenom prostoru samo ako je osiguran video nadzor prostorije.
Ukoliko se vanjskoj tvrtki prepušta održavanje opreme i aplikacija s povjerljivim podacima, Odjel može od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije Odjela radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti Odjel.
Odjel zadržava pravo da osobama koje se predstavljaju kao djelatnici vanjskih tvrtki uskrati pristup ukoliko nisu na popisu ovlaštenih djelatnika. Vanjska tvrtka je dužna najaviti svaku svoju aktivnost ili intervenciju IT službi Odjela najmanje 24 sata prije aktivnosti.

Sigurnosne kopije

Članak 29.

Računala s podacima važnim za rad i poslovanje Odjela moraju imati sigurnosne (rezervne) kopije podataka. Računala sa sigurnosnim kopijama i način njihovog pohranjivanja određuje Pročelnik u dogovoru s voditeljima stručnih službi. IT služba na zahtjev voditelja stručnih službi realizira pohranjivanje sigurnosnih kopija.

Korisnici studenti

Članak 30.

Korisnici studenti mogu koristi računala u knjižnici, računalnim učionicama i hodnicima.

Nije dozvoljeno spajanje osobnih računala studenata na fiksnu računalnu mrežu Odjela bez dozvole IT službe Odjela.

Nije dozvoljeno korištenje računala u računalnim učionicama bez dozvole nastavnika ili prisustva odgovorne osobe.

Nije dozvoljeno bilo kakvo mijenjanje postavki na računalima bez dozvole nastavnika, mijenjanje ili brisanje dokumenata i podataka s računala u prostorima Odjela.

Korištenje poslužitelja Odjela

Članak 31.

Svi djelatnici, vanjski suradnici i studenti Odjela mogu dobiti elektroničku adresu i diskovni prostor na nekom od poslužitelja Odjela.

Također, svi korisnici dobivaju elektronički identitet unutar sustava AAI@EduHr. Sve informacije o ovom sustavu mogu se naći na www.aaiedu.hr

Korisnička imena i pripadajuće lozinke su privatni i povjerljivi podaci i ne smiju se davati na korištenje drugim osobama. Vlasnik korisničkih podataka je odgovoran za svako njihovo korištenje čak i u slučaju da do tih podataka dođu druge osobe.

Ukoliko korisnik posumnja da su njegovi korisnički podaci kompromitirani, dužan je hitno se javiti IT službi.

Članak 32.

Svi korisnici obavezni su poštivati prava ostalih korisnika na poslužiteljima i to na način da odgovorno koriste raspoloživi diskovni prostor poslužitelja tj. da redovito brišu nepotrebne dokumente i elektroničku poštu.

Poslužitelje Odjela u pravilu održava IT služba, ali ona nije odgovorna za korisničke podatke i njihov sadržaj.

Zabranjeno je bilo kakvo brisanje ili mijenjanje podataka ili dokumenata bez dozvole vlasnika. IT služba zadržava pravo brisanja korisničkih dokumenata i podataka ukoliko oni ometaju rad drugih korisnika ili normalan rad poslužitelja.

Članak 33.

Odsjeci, zavodi i djelatnici mogu imati svoje poslužitelje. U tom je slučaju potrebno predati pismeni zahtjev za nabavu poslužitelja, a on mora sadržavati razloge za nabavu te ime osobe koja će ga održavati. Administratorska lozinka mora biti pohranjena u IT službi.

Odjel ne dozvoljava ostvarivanje korisničkih prava trećim osobama na poslužiteljima pod svojom domenom i računalnom mrežom.

Članak 34.

Odjel može objaviti statističke podatke o sigurnosnim incidentima samo ako ti podaci neće ugroziti privatnost korisnika, otkriti povjerljive podatke ili narušiti sigurnost i integritet informacijskog sustava.

Stegovne mjere

Članak 35.

Svi korisnici informatičkih usluga, vanjski suradnici i osobe koje na bilo koji način koriste informacijski sustav Odjela, dužni su pridržavati se pravila i procedura propisanih ovim Pravilnikom.
Da li je u pojedinom slučaju došlo do kršenja pravila o sigurnosti informacijskih sustava utvrdit će Povjerenstvo za sigurnost.
U slučaju kršenja sigurnosnih pravila protiv prekršitelja se može pokrenuti stegovni postupak.

Članak 36.

Vanjskim suradnicima i osobama koje nisu zaposlenici ni studenti Odjela, a na bilo koji način zloupotrebe informacijski sustav Odjela, može se trajno ili privremeno uskratiti pristup opremi i podacima, te razvrgnuti ugovor. Odjel je dužan u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.
Studentima koji krše pravila može se na određeno vrijeme ili trajno uskratiti pravo korištenja CARNetove mreže i usluga. O izricanju takve kazne mora se obavijesti CARNetov CERT. Pročelnik Odjela na temelju odluke Povjerenstva za sigurnost može donijeti odluku o drugim stegovnim mjerama za studente.
Ukoliko zaposlenici vanjskih tvrtki koji po ugovoru obavljaju poslove za Odjel krše sigurnosna pravila, Odjel im može zabraniti fizički pristup prostorijama ili pristup podacima. Odjel je dužan u ugovore s vanjskim tvrtkama ugraditi stavku po kojoj kršenje sigurnosne politike Odjela predstavlja dovoljan razlog za raskid ugovora.

Prijelazne i završne odredbe

Članak 37.

Ovaj Pravilnik stupa na snagu osmog dana od dana objavljivanja na oglasnim pločama Odjela.

Pročelnik Odjela

Dr. sc. Ado Matoković