Na temelju odredbe članka 24. Zakona o informacijskoj sigurnosti (NN 79/07) te odredbe članka 22. Statuta Europske poslovne škole Zagreb, Upravno vijeće Europske poslovne škole Zagreb (dalje: EBUS), donosi:

PRAVILNIK O SIGURNOSTI INFORMACIJSKIH SUSTAVA

Uvodne odredbe

Članak 1.

(1) Ovim se pravilnikom uređuje sigurnost upravljanja informacijskim sustavima na EBUS-u, definiraju prihvatljivi načini ponašanja i jasna raspodjela uloga i odgovornosti svih čimbenika informacijskog sustava.

(2) Postojeći zaposlenici i vanjski suradnici EBUS-a dužni su se upoznati s njegovim odredbama nakon njegovog stupanja na snagu.

(3) Novi zaposlenici EBUS-a, kao i vanjski suradnici EBUS-a dužni su se upoznati s njegovim odredbama prilikom zapošljavanja, a studenti prilikom otvaranja korisničkih računa.

(4) Pravila rada i ponašanja koja su definirana sigurnosnom politikom odnose se na:

- svu računalnu opremu koja se koristi u prostorima EBUS-a,
- 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 EBUS-a (u nastavku IT služba), ovlašteni CARNet sistem inženjeri te stručni suradnici ovlašteni od strane IT službe EBUS-a
- 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 EBUS-a, vanjski suradnici i studenti.
- glavni korisnik – osoba odgovorna za rad pojedine aplikacije u okviru informacijskog sustava, a koja je od vitalne važnosti za EBUS ili neki njegov dio.
- voditelj IT službe - osoba odgovorna za pravovremeno i redovito ažuriranje svih informacija koje se postavljaju na javne servise za informiranje.
- zona javnih servisa - oprema koja obavlja javne servise EBUS-a. U ovu opremu svrstavaju se: DNS poslužitelj, HTTP poslužitelj, poslužitelj elektroničke pošte, FTP poslužitelj itd...
- intranet - privatna mreža EBUS-a 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, Zstudent, X-ice, baze knjižnice, Zen) i sl.
- prijenosna računalna oprema - sastoji se od prijenosnih računala u vlasništvu EBUS-a koja

zaposlenici koriste izvan prostora EBUS-a i u prostoru EBUS-a. Takvu računalnu opremu zaposlenici EBUS-a smiju priključivati na fiksnu lokalnu mrežu samo na za to predviđenim mjestima i uz prethodnu suglasnost IT službe EBUS-a.

Organizacija upravljanja sigurnošću

Članak 3.

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

(2) Davatelji informatičkih usluga odgovaraju za ispravnost i neprekidnost rada informacijskog sustava. Samo davatelji smiju biti administratori računala koja se koriste na EBUS-u.

(3) IT služba EBUS-a može iznimno, na opravdani zahtjev korisnika ili uprave EBUS-a, 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.

(4) 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 EBUS-a i Pravilnikom o sigurnosti informacijskih sustava
- prijaviti svaki sigurnosni incident,
- izabrati kvalitetnu zaporku i povremeno je mijenjati te
- 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.

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

(2) Glavnog korisnika aplikacije imenuje dekan EBUS-a na temelju specifičnosti pojedine aplikacije i odgovornosti zaposlenika, a na prijedlog voditelja IT službe EBUS-a.

(3) Glavni korisnik je u pravilu voditelj određene službe ili nositelj nekog projekta.

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

(5) 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.

(6) Podatke o glavnim korisnicima pojedine vitalne aplikacije dužna je voditi IT služba EBUS-a.

Prihvatljivo korištenje računalne i mrežne opreme

Članak 6.

(1) Računalna i mrežna oprema EBUS-a, CARNet mreža i sve dostupne usluge na raspolaganju su korisnicima radi obavljanja posla, odnosno učenja, poučavanja i istraživanja.
Ova prava korisnici su dužni ostvarivati poštujući potrebe i prava ostalih korisnika.

(2) Sve ustanove spojenih na CARNet mrežu, kao i njihovi korisnici, dužni su se odgovorno i ponašati i koristiti informacijske resurse. Prihvatljivo korištenje računalne mreže EBUS-a 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 EBUS, ustanovu, CARNet, ostale ustanove članice CARNet mreže i bilo koje treće osobe.

Članak 8.

(1) 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 EBUS-a 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.

(2) Ukoliko nije siguran glede prava i načina upotrebe neke usluge, korisnik je dužan obratiti se IT službi EBUS-a

(3) 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 te
- 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 EBUS-a mogu se priključiti na računalnu mrežu Odjela isključivo uz odobrenje IT službe EBUS-a. U tom slučaju ti se korisnici moraju pridržavati svih pravila iz ovog dokumenta, a njihova računala moraju udovoljavati svim pravilima.

Članak 11.

(1) Voditelj IT službe EBUS-a zadužen je za provođenje hitnih mjera i poduzimanje sigurnosnih mjera u slučaju potrebe hitne intervencije.

(2) 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 EBUS-a.

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

Članak 12.

Voditelj IT službe EBUS-a 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 13.

(1) Voditelj IT službe E B U S - a poduzima radnje uz pomoć kojih otklanja posljedice incidenta na najbrži mogući način.

(2) Po otklanjanju incidenta voditelj IT službe EBUS-a izvještava dekana o incidentu, poduzetim mjerama te o potrebi poduzimanja daljnjih mjera.

(3) U slučaju težeg incidenta voditelj IT službe EBUS-a sačinjava izvješće o sigurnosnoj situaciji koje predaje dekanu EBUS-a.

Članak 14.

(1) Voditelj IT službe EBUS-a, na temelju izvješća o sigurnosnoj situaciji predlaže mjere za poboljšanje sigurnosti (nabava sigurnosne opreme i softvera, obrazovanje korisnika...).

(2) Voditelj IT službe EBUS-a provodi istragu u slučaju sigurnosnog incidenta i predlaže dekanu EBUS-a donošenje odluke o mjerama za sankcioniranje odgovornih korisnika.

(3) U slučaju sigurnosnog incidenta prouzrokovanog od strane osoba koje nisu korisnici EBUS-a, voditelj IT Službe EBUS-a daje CARNet koordinatoru nalog za prijavu sigurnosnog incidenta CERT-u koji se nalazi u sastavu CARNet-a.

Administriranje računala

Članak 15.

(1) IT služba EBUS-a dužna je administrirati računala i mrežnu opremu u skladu s pravilima struke, brinući istovremeno o funkcionalnosti i sigurnosti.

(2) 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 16.

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

(2) 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 17.

(1) 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.

(2) 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 18.

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 EBUS-a na nijedan način nije odgovorna za takva računala.

Instalacija i licenciranje softvera

Članak 19.

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 20.

IT služba EBUS-a 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 21.

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 22.

(1) Nadzor smiju obavljati samo osobe ovlaštene od strane EBUS-a. U pravilu su to djelatnici IT službe EBUS-a.

(2) Pri provođenju nadzora ovlaštene osobe su dužne poštivati privatnost korisnika te povjerljivost podataka i informacija.

(3) 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 23.

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 24.

(1) Prostor na EBUS-u se dijeli na dio koji je otvoren za javnost, prostor u koji imaju pristup samo zaposlenici EBUS-a te prostore u koje imaju pristup isključivo grupe zaposlenika, ovisno o vrsti posla koje obavljaju.

(2) EBUS je dužan sastaviti popis osoba koje imaju pravo pristupa u zaštićena područja, a porta mora imati popis osoba koje mogu dobiti ključeve određenih prostorija.

Članak 25.

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

(2) EBUS je dužan napraviti popis ovlaštenih osoba koje imaju pristup sigurnim zonama. U pravilu su to djelatnici IT službe EBUS-a koji administriraju poslužitelje i mrežnu opremu.

Članak 26.

Povremeno se u sigurnim prostorima mora dopustiti pristup osobama iz vanjskih tvrtki ili ustanova, radi servisiranja, održavanja, podrške, obuke, zajedničkog poslovanja itd. EBUS će 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 27.

(1) 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.

(2) Ukoliko se vanjskoj tvrtki prepušta održavanje opreme i aplikacija s povjerljivim podacima, EBUS može od vanjske tvrtke zatražiti popis osoba koje će dolaziti u prostorije EBUS-a radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti EBUS.

(3) EBUS 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 EBUS-a najmanje 24 sata prije aktivnosti.

Sigurnosne kopije

Članak 28.

Računala s podacima važnim za rad i poslovanje Odjela moraju imati sigurnosne (rezervne) kopije podataka. Računala sa sigurnosnim kopijama i način njihovog pohranjivanja određuje voditelj IT službe EBUS-a. IT služba na zahtjev realizira pohranjivanje sigurnosnih kopija.

Korisnici studenti

Članak 29.

(1) Korisnici studenti mogu koristi računala u knjižnici, računalnim učionicama, predavaonicama i hodnicima.

(2) Nije dozvoljeno spajanje osobnih računala studenata na fiksnu računalnu mrežu Odjela bez dozvole IT službe EBUS-a.

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

(4) Nije dozvoljeno bilo kakvo mijenjanje postavki na računalima bez dozvole nastavnika, mijenjanje ili brisanje dokumenata i podataka s računala u prostorima EBUS-a.

Korištenje poslužitelja EBUS-a

Članak 30.

(1) Svi djelatnici, vanjski suradnici i studenti EBUS-a mogu dobiti elektroničku adresu i diskovni prostor na nekom od poslužitelja EBUS-a.

(2) Svi korisnici dobivaju elektronički identitet unutar sustava AAI@EduHr. Sve informacije o ovom sustavu mogu se naći na www.aaiedu.hr

(3) 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.

(4) Ukoliko korisnik posumnja da su njegovi korisnički podaci kompromitirani, dužan je hitno se javiti IT službi EBUS-a.

Članak 31.

(1) 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.

(2) Poslužitelje EBUS-a u pravilu održava IT služba EBUS-a, ali ona nije odgovorna za korisničke podatke i njihov sadržaj.

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

Članak 32.

(1) Ustrojstvene jedinice EBUS-a 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 EBUS-a.

(2) EBUS ne dozvoljava ostvarivanje korisničkih prava trećim osobama na poslužiteljima pod svojom domenom i računalnom mrežom.

Članak 33.

EBUS 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 34.

(1) Svi korisnici informatičkih usluga, vanjski suradnici i osobe koje na bilo koji način koriste informacijski sustav EBUS-a, dužni su pridržavati se pravila i procedura propisanih ovim Pravilnikom.

(2) Slučajeve kršenja pravila o sigurnosti informacijskih sustava utvrđuje IT služba EBUS-a.

(3) U slučaju kršenja sigurnosnih pravila protiv prekršitelja se može pokrenuti stegovni postupak.

Članak 35.

(1) Vanjskim suradnicima i osobama koje nisu zaposlenici niti studenti EBUS-a, a na bilo koji način zloupotrebe informacijski sustav EBUS-a, može se trajno ili privremeno uskratiti pristup opremi i podacima, te razvrgnuti ugovor. EBUS je dužan u ugovor unijeti stavke po kojima je povreda povjerljivosti podataka dovoljan razlog za prekid ugovora.

(2) 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. Voditelj IT službe EBUS-a predaže stegovne mjere za studente.

(3) Ukoliko zaposlenici vanjskih tvrtki, koji po ugovoru obavljaju poslove za EBUS, krše sigurnosna pravila, EBUS im može zabraniti fizički pristup prostorijama ili pristup podacima. EBUS je dužan u ugovore s vanjskim tvrtkama ugraditi stavku po kojoj kršenje sigurnosne politike EBUS-a predstavlja dovoljan razlog za raskid ugovora.

Prijelazne i završne odredbe

Članak 36.

Ovaj Pravilnik stupa na snagu danom donošenja, a objavljuje se na oglasnoj ploči EBUS-a i web stranici EBUS-a.

KLASA: 602-04/20-10/31
URBROJ: 251-478-01-21-02
Zagreb, 12.03.2021.

EUROPSKA POSLOVNA ŠKOLA ZAGREB
ZAGREB

Za Upravno vijeće:

Vitomir Tafra, mag. oec.