Na temelju članka 24. Zakona o informacijskoj sigurnosti („Narodne novine“ broj 79/07 i 14/24), članka 26. Statuta Ekonomskog fakulteta u Splitu te Politike informacijske sigurnosti Ekonomskog fakulteta u Splitu, u skladu s odredbama Pravilnika o radu Ekonomskog fakulteta u Splitu, nakon savjetovanja sa službenicima za zaštitu osobnih podataka Ekonomskog fakulteta u Splitu, dekan prof. dr. sc. Bruno Ćorić, dana 03. prosinca 2024. godine, donio je

PRAVILNIK
o računalnoj sigurnosti
Ekonomskog fakulteta u Splitu

Uvodne odredbe

Članak 1.

(1) Ovim se Pravilnikom o računalnoj sigurnosti Ekonomskog fakulteta u Splitu (dalje u tekstu: Pravilnik) uređuje sigurnosna politika informacijskog (računalnog) sustava na Ekonomskom fakultetu u Splitu (dalje u tekstu: Fakultet), na način da se definiraju prihvatljivi načini ponašanja u svezi korištenja informacijskog sustava Fakulteta, raspoređuju zadatci i odgovornosti nadležnih osoba te propisuju sankcije u slučaju nepridržavanja njegovih odredbi, s ciljem zaštite informacija i podataka koji se u sustavu kreiraju, prenose, pohranjuju i obrađuju te zaštite investicije Fakulteta u računalni sustav.
(2) Ovaj Pravilnik primjenjuje se na radnike, vanjske suradnike i studente Fakulteta koji koriste informacijski sustav Fakulteta te kojima je njegova upotreba dopuštena.
(3) Ne postupanje radnika po odredbama ovog Pravilnika smatra se povredom radnih i drugih obveza radnika iz rada i u vezi s njim te podliježe stegovnoj odgovornosti prema odredbama posebnog pravilnika Fakulteta.
(4) Pravilnik obuhvaća informacijski sustav Fakulteta i sve sadržaje koji se prenose, pohranjuju i obrađuju u tom sustavu, sadržaje pohranjene na svim osobnim računalima u vlasništvu Fakulteta, kao i sve poslužitelje koji su u administrativnoj domeni ili vlasništvu Fakulteta.

Članak 2.

U smislu ovog Pravilnika:

- **Korisnik** je svaka osoba koja koristi informatičku opremu i informacijski sustav u vlasništvu Fakulteta.
- **Administrator informacijske sigurnosti** (dalje u tekstu: Administrator) je osoba odgovorna za informacijsku sigurnost na Fakultetu.
- **Davatelji usluga** su profesionalci koji se brinu o radu računala, mreže i informacijskih sustava i to osobe koje su za to zaposlene na odgovarajućim radnim mjestima Fakulteta te vanjske osobe s kojima je sklopljen odgovarajući ugovor za održavanje informacijskog sustava Fakulteta. Davatelji usluga odgovaraju za ispravnost i neprekidnost rada informacijskog sustava.
- **Povjerenstvo za sigurnost** informacijskog sustava imenuje dekan s ciljem kvalitetnijeg sveukupnog upravljanja informacijskom sigurnošću Fakulteta.
- **Server-soba** je odvojeni prostor za smještaj računalne opreme koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskog sustava ili sadrži povjerljive informacije u tom sustavu.
- **Poslužitelj** je informacijski sustav koji obuhvaća jedan ili više sustava za računalnu potporu poslovnih procesa (računovodstvo, kadrovski poslovi, upravljanje studentima (ISVU) i sl.).

Odgovornost

Članak 3.

(1) Za primjenu ovog Pravilnika i korištenje informatičke opreme u vlasništvu Fakulteta odgovorna je osoba kojoj su ugovorom o radu ili posebnom odlukom dekana povjereni poslovi brige o informacijskoj sigurnosti Fakulteta (dalje u tekstu: administrator informacijske sigurnosti).

(2) Osobe zaposlene na poslovima brige o razvoju i održavanju informacijskih sustava Fakulteta (dalje: osobe na informatičkim poslovima), sukladno i u opsegu obveza i ovlaštenja dodijeljenih im ugovorom o radu, odgovorne su za:

- administriranje i održavanje sigurnosti informacijskog sustava, što uključuje materiju koju uređuje ovaj Pravilnik te 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.

Voditelji ustrojstvenih jedinica obvezni su u njima 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.

(3) Fakultet štiti svoju računalnu opremu, sklopovlje, programsku podršku, podatke i dokumentaciju od zlouporabe, krađe, neovlaštene uporabe i upliva okoliša. Za sigurnost informacijskog sustava Fakulteta odgovorni su korisnici i administrator informacijske sigurnosti, svaki u svom dijelu odgovornosti propisane ovim Pravilnikom.

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

(5) Administrator informacijske sigurnosti odgovoran je da sva kritična računalna oprema bude priključena na izvore neprekidnog napajanja, a ostala oprema da bude zaštićena prednaponskom zaštitom. Osobe na informatičkim poslovima, u okviru svojih ovlaštenja, odgovorne su za sve instalacije, odspajanja, promjene i premještanje računalne opreme. Korisnici ne smiju samostalno poduzimati takve radnje, što se ne odnosi na prijenosna računala za koja su početnu konfiguraciju i priključenje u sustav obavile osobe na informatičkim poslovima, u okviru svojih ovlaštenja.

(6) U pogledu informacijske sigurnosti korisnici su obvezni pridržavati se uputa:

- Mediji s podacima i programskom podrškom (CD-ovi, 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 biti čuvani podalje od nepovoljnih utjecaja okoliša, kao što su toplina, direktno sunčevo svjetlo, vlaga i elektromagnetska polja i sl.
- 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 Fakulteta bez odobrenja administratora informacijske 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.

Povjerenstvo za sigurnost informacijskog sustava

Članak 4.

(1) Povjerenstvo za sigurnost informacijskog sustava (dalje u tekstu: Povjerenstvo) imenuje dekan odlukom, na prijedlog administratora informacijske sigurnosti.
(2) Članovi Povjerenstva su: administrator informacijske sigurnosti, predstavnik uprave, predstavnik vanjskog davatelja usluge (ako postoji) i predstavnik korisnika.
(3) Povjerenstvom predsjedava administrator informacijske sigurnosti.
(4) Povjerenstvo je obvezno:

- zaprimati izvještaje o sigurnosnoj situaciji i predlagati mjere za njeno poboljšanje, uključujući nabavu opreme, organizaciju obrazovanja korisnika i specijalista.
- pokretati istrage u slučaju incidenata, o njima sastavljati izvješća te ih po potrebi prijavljivati radi pokretanja stegovnog postupka, sukladno ostalim aktima Fakulteta
- upravi Fakulteta podnositi izvještaje o stanju sigurnosti, predlagati donošenje konkretnih mjera, nabavljanje potrebne opreme, te ulaganje u obrazovanje specijalista, ali i običnih korisnika.

(5) 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 i kao dokazni materijal u eventualnim stegovnim ili sudskim procesima.
(6) Ozbiljnije incidente dekan je dužan prijaviti CARNetovom CERT-u.

Administriranje korisnika

Članak 5.

(1) Osobe na informatičkim poslovima, u okviru svojih ovlaštenja, odgovorne su za administraciju kontrole pristupa u računalni informacijski sustav, što uključuje dodavanje, brisanje i promjene prava pristupa korisnicima.
(2) Administracija korisnika se temelji na zahtjevima:

- Studentske referade za studente i
- prodekana i voditelja ustrojstvene jedinice u čijoj je organizacijskoj nadležnosti korisnik.

(3) Zahtjev se dostavlja putem obrasca koji je sastavni dio aplikacije Epredlošci. U slučaju hitnosti, brisanja i zabrane prava pristupa mogu se izvršiti i na usmeni zahtjev nadležnog voditelja ustrojstvene jedinice, nakon čega mora slijediti i pisani zahtjev kao potvrda.
(4) Studentska referada obvezna je za svakog studenta koji gubi status studenta završetkom ili prekidom studija, najkasnije 15 dana od prestanka statusa studenta, administratoru informacijske sigurnosti dostaviti zahtjev za brisanje korisnika. Prodekan za nastavu i studentska pitanja obvezan je za svakog nastavnika i suradnika kojem po bilo kojoj osnovi prestaje nastavna djelatnost na Fakultetu, a najkasnije 15 dana od prestanka, administratoru informacijske sigurnosti dostaviti zahtjev za brisanje korisnika.
(5) Voditelji ustrojstvenih jedinica prestanak radnog odnosa radnika iz svoje ustrojstvene jedinice moraju prijaviti administratoru informacijske sigurnosti istodobno s dokumentom o prestanku radnog odnosa, kako bi njihova pristupna prava i zaporke bili opozvani ili izmijenjeni.
(6) Korisnik osobnog računala za potrebe korištenja istog osobnog računala od strane druge osobe (demonstrator, vanjski suradnik i dr.) može zatražiti otvaranje lokalnog korisničkog računa na računalu koje koristi.

Administriranje računalne opreme

Članak 6.

(1) Svako računalo u vlasništvu Fakulteta mora imati imenovanog administratora, koji odgovara za instalaciju i konfiguraciju softvera.
(2) Administrator informacijskog sustava može naprednim korisnicima odobriti da sami administriraju svoje osobno računalo.
(3) 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).
(4) Davatelji usluga dužni su u svome radu poštivati privatnost ostalih korisnika i povjerljivost informacija s kojima dolaze u dodir pri obavljanju posla.
(5) Administratori su dužni prijaviti incidente administratoru informacijskog sustava te pomoći pri istrazi i uklanjanju problema. Incidente treba dokumentirati kako bi se pomoglo u nastojanju da se izbjegnu slične situacije u budućnosti.
(6) Administratorska prava na računalima koja koriste više osoba mogu imati samo osobe na informatičkim poslovima.
(7) Administratorska prava na osobnim računalima za osobne potrebe mogu biti dodijeljena i samom korisniku, ukoliko administrator informacijskog sustava procijeni da je on stručno sposoban samostalno administrirati računalo na osobnom korištenju, a na svim ostalim osobnim računalima administratorska prava mogu imati samo osobe na informatičkim poslovima, sukladno svojim ovlaštenjima.

Upravljanje računalnom mrežom

Članak 7.

(1) Upravljanje računalnom mrežom u nadležnosti je isključivo osoba na informatičkim poslovima, sukladno njihovim ovlaštenjima, kao i ugovornih vanjskih davatelja usluge održavanja računalne mreže (ako takvi postoje).
(2) Osobe na informatičkim poslovima, sukladno svojim ovlaštenjima, moraju ažurno voditi dokumentaciju o cjelokupnoj računalnoj mreži Fakulteta, koja se obvezno treba čuvati u metalnom ormaru (sefu) u vrijeme kad se ne koristi.
(3) Ukoliko je dokumentacija o računalnoj mreži u digitalnom formatu, administrator informacijskog sustava je obvezan propisati način sigurnog korištenja za davatelje usluge.
(4) Osobe na informatičkim poslovima, sukladno svojim ovlaštenjima, moraju u svakom trenutku imati točan popis svih mrežnih priključaka i umreženih uređaja, uključujući i prenosiva računala.
(5) Na prijedlog administratora informacijskog sustava Fakultet treba propisati pravila za spajanje na računalnu žičnu i bežičnu mrežu Fakulteta gostujućih računala, koja donose sa sobom vanjski suradnici, predavači, poslovni partneri i serviseri.

Zaporke i pristupni računi

Članak 8.

(1) Zabranjeno je korištenje grupnih i univerzalnih pristupnih računa za pristup računalima i računalnim sustavima Fakulteta.
(2) Svaka osoba obvezno mora pristupiti računalnom sustavu i računalima Fakulteta isključivo vlastitim pristupnim računom.
(3) Izuzetno, administrator informacijske sigurnosti može na pisano traženje dekana ili prodekana odobriti korisniku korištenje pristupnog računa druge osobe za pronalaženje i

otklanjanje nepravilnosti rada sustava, o čemu treba načiniti pisani dokument. Nakon završetka ovih radnji obavezno treba promijeniti zaporku toga pristupnog računa.

Postupak sa zaporkama

Članak 9.

(1) Korisnik:

- je odgovoran za sve računalne transakcije učinjene korištenjem dodijeljenog mu prijavnog imena i zaporke
- osim u propisanim slučajevima, sukladno odlukama dekana, 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 koristiti zaporke koje nije lako pogoditi
- treba se odjaviti iz informacijskog sustava kada napušta radno mjesto.

(2) Svi korisnici dužni su administratoru informacijske sigurnosti dostaviti sve administratorske zaporke kojima se, kao radnik Fakulteta, koristi. Administrator informacijske sigurnosti obvezan je sve administratorske zaporke pohraniti u adekvatni metalni ormar (sef) koji treba uvijek držati zaključanim, čiji ključ mora imati administrator informacijske sigurnosti te dekan, za slučaj njegove nedostupnosti.

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

(4) Korisnik je obvezan nakon svake promjene, unutar jednog radnog dana, ažurirati pohranjene zaporke. Pored pohranjenih zaporki, treba pohraniti i detaljno dokumentirane upute kako doći do kritičnih podataka na poslužiteljima.

Računalni virusi

Članak 10.

(1) Računalni virusi i drugi zloćudni programi (dalje u tekstu: virusi) su programi načinjeni sa svrhom da čine neovlaštene promjene na podatcima i aplikacijama, koji mogu nanijeti štetu Fakultetu.

(2) Obrana protiv virusa uključuje zaštitu od neovlaštenog pristupa računalnim resursima, uporabu samo provjerenih izvora podataka i programske zaštite te održavanje ažurnosti sustava za detekciju i uklanjanje virusa.

(3) U pogledu zaštite od virusa uprava Fakulteta je obvezna u svom proračunu redovito osiguravati dostatna financijska sredstva za nabavku i održavanje programske i sklopovske opreme za zaštitu od njih.

(4) U pogledu zaštite od virusa, osobe na informatičkim poslovima, sukladno svojim ovlaštenjima, obvezne su:

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

(5) U pogledu zaštite od virusa, obveze korisnika su:

- ne smiju svjesno unijeti virus u računalni sustav Fakulteta
- trebaju izbjegavati internetske stranice na kojima se pružaju nelegalne usluge, piratske kopije računalnih programa i audio/video sadržaja te moralno neprimjereni sadržaj
- ne smiju na računalima Fakulteta rabiti podatkovne medije nepoznatog porijekla i sadržaja

- trebaju sami ili uz pomoć stručne osobe antivirusnim programom, odobrenim od strane administratora informacijske sigurnosti, pregledati medije koji se prije njihove upotrebe unose
- ukoliko posumnja da je njegovo računalo zaraženo virusom ili da antivirusna zaštita nije aktivna ili ažurna, korisnik mora računalo odmah isključiti i prijaviti zapažanje administratoru informacijske sigurnosti.

Intelektualno vlasništvo i licenčna prava

Članak 11.

(1) Obveza je Fakulteta i svih radnika da poštuju zakone i propise o zaštiti intelektualnog vlasništva. Fakultet je obvezan koristiti programsku podršku na temelju valjanih licenčnih prava. Fakultet programsku podršku i pripadajuću dokumentaciju koja nije u vlasništvu Fakulteta nema pravo umnožavati i/ili distribuirati bez dopuštenja proizvođača ili autora, osim za potrebe stvaranja sigurnosne kopije.
(2) Na računalima u vlasništvu Fakulteta ne smije se bez odobrenja administratora informacijske sigurnosti koristiti programska podrška nabavljena privatno, bilo kupnjom ili donacijom.
(3) Legalnost licenci donirane programske podrške utvrđuje se posebnim ugovorom.
(4) Osobe na informatičkim poslovima, sukladno svojim ovlaštenjima, dužne su:
- održavati ažuran popis programskih licenci u vlasništvu Fakulteta
- čuvati licenčne ugovore ili uvjete korištenja programske potpore
- periodički, metodom slučajnog odabira, pregledati računala u vlasništvu Fakulteta radi provjere uporabe samo legalne programske podrške.

(5) Korisnici ne smiju:
- koristiti programsku podršku na način koji nije u skladu s licenčnim pravima proizvođača
- instalirati aplikacije koje nije odobrio administrator informacijske sigurnosti na računala u vlasništvu Fakulteta
- na računala u vlasništvu Fakulteta instalirati programsku podršku koja nije licencirana ili nije u vlasništvu Fakulteta
- kopirati programsku podršku bez prethodnog odobrenja administratora informacijske sigurnosti
- preuzimati programsku podršku s Interneta bez prethodnog odobrenja administratora informacijske sigurnosti.

Fizička zaštita

Članak 12.

(1) Računalna oprema koja obavlja kritične funkcije, neophodne za funkcioniranje informacijskog sustava Fakulteta ili sadrži povjerljive informacije, fizički se odvaja u prostor (podatkovni centar) u koji je ulaz dozvoljen samo ovlaštenim osobama.
(2) Ulazak osoba u podatkovni centar treba biti strogo kontroliran. Dekan ili administrator informacijske sigurnosti odobravaju popis osoba koje mogu ulaziti u pojedine dijelove podatkovnog centra.
(3) Ulazak osoba u podatkovni centar osoba koje nisu na popisu iz prethodnog stavka ovog članka može biti jednokratno pisano odobren od strane administratora informacijske 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 osoba na informatičkim poslovima. Ulazak tih osoba obvezno se evidentira u dnevniku ulaska osoba u podatkovni centar.

(4) 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 zapaljivih i eksplozivnih stvari i materijala.
(5) Ukoliko Fakultet prepušta vanjskoj tvrtki održavanje opreme i aplikacija s povjerljivim podacima, administrator informacijske sigurnosti odobrava popis osoba vanjske tvrtke koje će dolaziti u prostorije podatkovnog centra Fakulteta radi obavljanja posla. U slučaju zamjene izvršitelja, vanjska tvrtka dužna je na vrijeme obavijestiti Fakultet. Fakultet zadržava pravo da osobama koje se predstavljaju kao radnici vanjskih tvrtki uskrati pristup ukoliko nisu na popisu ovlaštenih radnika.

Fizička sigurnost opreme

Članak 13.

(1) U prostorijama Fakulteta nalazi se informatička oprema u vlasništvu Fakulteta, oprema u najmu drugih vlasnika i oprema CARNeta, koja je dana na korištenje Fakultetu.
(2) Za fizičku sigurnost opreme na Fakultetu odgovoran je dekan, koji odgovornost za grupe uređaja ili pojedine uređaje može prenijeti na druge radnike Fakulteta, koji potpisuju dokument kojim potvrđuju da su preuzeli opremu.
(3) Administrator informatičke sigurnosti ili druga osoba po odluci dekana odgovorna je za održavanje ažurnog popisa sve računalne opreme, s popisom ugrađenih glavnih modula komponenti, inventarskim brojevima itd.

Neprekidnost poslovanja

Članak 14.

(1) Kako bi se sačuvali podatci u slučaju nezgoda, poput kvarova na sklopovlju, požara, ili ljudskih grešaka, potrebno je redovito izrađivati rezervne kopije svih vrijednih informacija, uključujući i konfiguraciju softvera.
(2) Preporučuje se izrada više kopija, koje se čuvaju na različitim mjestima, po mogućnosti u vatrootpornim ormarima. Izrada kopija on-line preko zasebne računalne mreže ili Interneta obvezno se treba izvoditi primjenom adekvatnog sustava kriptiranja podataka u prijenosu.
(3) Fakultet 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.

Završne odredbe

Članak 15.

Ovaj Pravilnik stupa na snagu osmog dana od dana objave na mrežnim stranicama Fakulteta.

DEKAN:

Prof. dr. sc. Bruno Ćorić

KLASA: 650-02/24-01/01
UR.BROJ: 2181-196-01-01-24-01
Split, 03. prosinca 2024.