UNIVERZITET UNIVERSITY

FINRA

TUZLA

unique blend of theory and practice

PRAVILNIK
O UPOTREBI I SIGURNOSTI INFORMACIONOG SISTEMA UNIVERZITETA FINRA Tuzla

Decembar, 2024. godine

Na osnovu člana 63. Zakona o visokom obrazovanju Tuzlanskog kantona („Službene novine Tuzlanskog kantona“, broj: 21/2021 - prečišćen tekst, 22/2021 - autentično tumačenje, 5/2022, 11/2022 i 16/2022) i člana 39. Statuta visokoškolske ustanove Univerziteta FINRA Tuzla, na 13. (trinaestoj) sjednici održanoj dana 26.12.2024. godine, Senat visokoškolske ustanove Univerziteta FINRA Tuzla (u daljem tekstu: Univerzitet), donosi:

PRAVILNIK
o upotrebi i sigurnosti informacionog sistema Univerziteta FINRA Tuzla

Član 1.
(Predmet regulisanja)

Ovim Pravilnikom se utvrđuju:

- ciljevi zaštite sigurnosti Informacionog sistema Univerziteta (IS),
- organizacija zaštite sigurnosti,
- mjere i sredstva zaštite sigurnosti,
- provođenje mjera i sredstava zaštite sigurnosti,
- odgovornost zbog nepridržavanja mjera i sredstava zaštite sigurnosti,
- završne odredbe.

Član 2.
(Terminologija)

Pojedini pojmovi koji se koriste u ovom Pravilniku imaju sljedeće značenje:

1. *Autentifikacija podataka* - postupak kod kojega se ispituje da li je korisnik (njegova poruka) autentična, tj. da li se radi upravo o poruci koja se očekuje. Potvrda da nitko nije nešto dodavao u poruku niti mijenjao poruku. Postupak je takav da se na strani pošiljatelja dodaje dodatna informacija poruci koja ovisi o sadržaju poruke, a na prijemnoj strani se to verificira.

2. *Autorizacija* - postupak kod kojega najčešće programska podrška (software) ispituje da li je oprema ili korisnik koji pristupa autoriziran, tj. da li mu je dozvoljen pristup.

3. *Autorizirani korisnik* - korisnik koji je uspješno »prošao« postupak autorizacije, tj. korisnik kojemu je sistem autorizacije dozvolio pristup.

4. *Lozinka (password)* - jedinstveni red znakova koje zna samo korisnik.

5. *Account* - mrežno ime ili identitet korisnika koji radi na računaru priključenom na LAN (računarsku mrežu).

6. *Korisnik* - korisnik informacionog sistema je osoba koja koristi računarsku opremu, računarske programe i baze podataka, koja razvija programe i aplikacije za podršku poslovnom procesu, koja kreira, organizira i održava baze podataka te koja koristi računar kao samostalnu radnu stanicu ili kao radnu stanicu na mreži.

7. *Administrator* - autorizirani korisnik sa specijalnim ovlastima za rad sa računarom, računarskim programima, bazama podataka, s ovlaštenjima pristupa do računara kao samostalne radne jedinice ili kao jedinice na mreži, a za potrebe administriranja i nadzora nad bazama podataka te administriranja, nadzora i upravljanja računarskom i mrežnom opremom.

8. *Firewall* - sigurnosna zaštita, filter koji ograničava pristup/prolaz neautoriziranim korisnicima za zaštitu lokalne mreže od neovlaštenog pristupa iz vanjskog svijeta te za sprečavanje nedozvoljenog prometa mrežom iznutra prema van.

9. *Elektronska pošta (e-mail)* - protokol na Internetu, koji omogućuva korisnicima slanje tekstualnih poruka s računara na računar. Kao dodatak tekstualnoj poruci mogu se poslati sve vrste dokumenata u elektronskom formatu: kolor fotografije, animacije, dokumenti itd.

10. *Elektronski zapis* - je cjelovit skup podataka koji su elektronski generirani, poslati, primljeni ili sačuvani na elektronskom, magnetnom, optičkom ili drugom mediju. Sadržaj elektronskog zapisa uključuje sve oblike pisanog i drugog teksta, podatke, slike i crteže, karte, zvuk, muziku, govor te računarske baze podataka.

11. *Virus* - kompjuterski virusi su kratki programi, čija je odlika brzo razmnožavanje, odnosno multipliciranje i izvršavanje određenih primarnih komandi, a virusi novije generacije prilikom kopiranja još i mutiraju, mijenjajući svoj osnovni source, odnosno prave štetu po sistemu.

12. *Softver* - softver ili programska podrška za rad računara je niz instrukcija i podataka pohranjenih u elektronskom obliku u računaru.

13. *Operativni sistem* – operativni sistem je skup osnovnih programa i alata koji pokreću računar, upravljaju svim procesima u računaru, fizičkim i programskim dijelovima računara te uređuju njihovu komunikaciju.

14. *Aplikacija* - aplikacija je program ili skup programa dizajniranih za pružanje podrške poslovnom procesu.

15. *Mreža* - mrežna infrastruktura za podršku informacionom sistemu obuhvaća sve mrežne resurse (servere baza podataka, web servere, servere za administriranje i nadzor mreže, za primanje i slanje elektronske pošte, ...), radne stanice s pripadajućom perifernom opremom, mrežnu i komunikacijsku opremu za povezivanje lokalnih radnih stanica u lokalne mreže i izdvojenih, dislociranih radnih stanica kojima se omogućuje pristup do zajedničkih baza podataka.

16. *Radna stanica* - računar s pripadajućom perifernom opremom na kojem korisnik koristi računarske programe i baze podataka, razvija programe i aplikacije za podršku poslovnom procesu, kreira, organizira i održava baze podataka, bez obzira da li ga koristi kao samostalnu radnu stanicu ili kao radnu stanicu na mreži.

17. *Serveri* - serveri su računari ili programski paketi koji omogućavaju specifičnu vrstu usluge za klijent programe koji se vrte na drugim računarima.

18. *Klijent* - klijent je računar koji otvara i koristi programe i aplikacije sa servera ili preuzima s njega programe i podatke.

19. *Licenca* – Pravo ili dozvola za korištenje određenog softvera za određeni vremenski period koji može biti i neograničen. Licencom se pored prava definiše i način i ostali uslovi korištenja softvera.

20. *Tajni podatak* - činjenica ili sredstvo koje se odnosi na javnu sigurnost, odbranu, vanjske poslove ili obavještajnu i sigurnosnu djelatnost Bosne i Hercegovine, koji je potrebno, u skladu s odredbama Zakona, zaštititi od neovlaštenih osoba i koji je ovlaštena osoba označila oznakom tajnosti.

I. CILJEVI ZAŠTITE SIGURNOSTI IS-a

Član 3.
(Ciljevi zaštite sigurnosti Informacionog sistema)

(1) Ciljevi zaštite sigurnosti Informacionog sistema u smislu ovoga Pravilnika su:
- očuvanje i zaštita integriteta IS-a Univerziteta;
- regulisanje dostupnosti podacima;
- zaštita povjerljivosti podataka; i
- čuvanje poslovne tajne.

Član 4.
(Zaštita Informacionog sistema)

(1) Informacioni sistem Univerziteta potrebno je štiti od:
- elementarnih nepogoda;
- požara;
- prekida ili neurednog napajanja električnom energijom;
- neovlaštenog pristupa i korištenja podataka i/ili programa;
- krađe opreme;
- krađe podataka i/ili programa;
- namjernog uništenja opreme i/ili podataka i/ili programa;
- zaraze računarskim virusom;
- neovlaštenog korištenja resursa;
- sprečavanja drugih u korištenju resursa;

- slučajnog gubitka podataka i/ili programa;
- kvara opreme;
- drugih okolnosti kojima se može ugroziti IS Univerziteta;

(2) Otklanjanje opasnosti iz stava 1 ovoga člana osigurava se utvrđivanjem organizacije zaštite sigurnosti, mjera i sredstava zaštite sigurnosti, provedbe mjera i sredstava zaštite sigurnosti te utvrđivanja odgovornosti zbog nepridržavanja mjera i sredstava zaštite sigurnosti.

Član 5.
(Očuvanje i zaštita integriteta)

(1) Informacioni sistem Univerziteta, u smislu ovoga Pravilnika, obuhvaća informacioni sistem i zajedničke baze podataka IS-a Univerziteta.

(2) Očuvanje i zaštita integriteta IS-a Univerziteta osigurava se primjenom ovoga Pravilnika nad svim informacionim sistemima i bazama podataka iz stava 1. ovoga člana.

Član 6.
(Dostupnost podacima Informacionog sistema)

(1) Dostupnost podacima IS-a Univerziteta utvrđuje se organizacijom, mjerama i sredstvima zaštite sigurnosti utvrđenim ovim Pravilnikom.

(2) Podaci, u smislu ovoga Pravilnika, su elektronski zapisi, dokumenti, njihovi sadržaji i prilozi, kao i usmena saopštenja i informacije povjerljive naravi, iznijeti u radu Univerziteta.

(3) Dokumenti, u smislu ovoga Pravilnika, su svi pisani akti (akti, tabele, grafikoni, nacrti, crteži, i slično).

Član 7.
(Tajni podatak)

(1) Tajni podatak - činjenica ili sredstvo koje se odnosi na javnu sigurnost, odbranu, vanjske poslove ili obavještajnu i sigurnosnu djelatnost Bosne i Hercegovine, koji je potrebno, u skladu s odredbama Zakona, zaštititi od neovlaštenih osoba i koji je ovlaštena osoba označila oznakom tajnosti.

(2) Tajnom se smatra i svaki podatak koji je zakonom, drugim propisom ili općim aktom Univerziteta u Tuzli određen kao tajni.

(3) Podaci iz stava 2. ovoga člana smatraju se tajnim bez obzira jesu li napisani rukom, osobnim računarom, strojem, štampani, stenografirani, šifrirani, filmirani, fotokopirani, snimljeni na magnetnoj traci, usb, hard diskovima, CD/DVD-u ili drugim medijima.

(4) Prije usmenog saopštenja tajnih podataka daje se prethodno upozorenje o tajnosti koje ima istu važnost kao i pisano utvrđena vrsta tajne i stepen tajnosti.

(5) Poslovnu tajnu predstavljaju podaci koji su kao poslovna tajna određeni zakonom, drugim propisom ili općim aktom Univerziteta.

Član 8.
(Dužnost čuvanja tajnih podataka)

(1) Tajne podatke su dužni čuvati svi zaposlenici i spoljni saradnici Univerziteta.

(2) Dužnost čuvanja tajnih podataka odnosi se na sve osobe iz prethodnog stava ovoga člana i nakon isteka njihovog mandata, prestanka radnog odnosa ili prestanka obavljanja poslova.

Član 9.
(Neovlašteno saopštenje tajnih podataka)

Za neovlašteno saopštenje tajnih podataka Univerzitet će postupiti u skladu sa Zakonom i općim aktom Univerziteta kojim se uređuje zaštita tajnosti podataka.

II. ORGANIZACIJA ZAŠTITE SIGURNOSTI

1. Područje obuhvata zaštite

Član 10.
(Područje obuhvata zaštite)

Organizacijom zaštite sigurnosti, u smislu ovoga Pravilnika, obuhvaćeni su:

- zgrade;
- prostorije;
- mrežna infrastruktura;
- serveri;
- radne stanice;
- operativni sistemi;
- aplikacije;
- podaci i baze podataka i
- neumreženi i drugi sistemi IS-a Univerziteta.

Član 11.
(Mjere i sredstva zaštite)

Mjere i sredstva zaštite sigurnosti IS-a Univeziteta utvrđene ovim Pravilnikom primjenjuju se nad svim objektima iz člana 10. ovoga Pravilnika.

2. Načini korištenja Informacionog sistema

Član 12.
(Način korištenja)

(1) Lični računari, samostojeći ili povezani u lokalne mreže, s pripadajućim programima i podacima, kao i ostala informatička oprema u vlasništvu Univeziteta smiju se koristiti isključivo za potrebe posla, i u okviru ovlaštenja za obavljanje poslova.

(2) Zabranjeno je koristiti lične računare i ostalu informatičku opremu, aplikacije i podatke izvan prostorija Univeziteta bez odobrenja ovlaštene osobe.

Član 13.
(Pravila za korištenje informatičke opreme)

Korisnici informatičke opreme dužni su pridržavati se pravila za korištenje informatičke opreme i provoditi sve predviđene procedure i tehničke upute za korištenje informatičke opreme.

Član 14.
(Tehnički zahvati)

(1) Tehničke zahvate na informatičkoj opremi (promjena konfiguracije, zamjena pojedinih dijelova opreme) smiju obavljati samo za to ovlaštene osobe koji su zaduženi za informatičku djelatnost ili ovlašteni serviseri uz nadzor administratora sistema ili osobe koja je za to ovlaštena odobrenjem Rektora Univerziteta, uz pisani nalog.

(2) Korisnicima informatičke opreme je zabranjeno obavljati tehničke zahvate iz prethodnog stava ovoga člana.

Član 15.
(Korištenje potrošnog materijala)

(1) Korisnik smije koristiti samo odgovarajući potrošni materijal (optičke medije, papir, tinte za pisače i slično) kako ne bi nastale štete na informatičkoj opremi.

(2) Prilikom javne nabavke informatičke opreme i potrošnog materijala obavezno konsultovati administratora odnosno za to ovlaštene osobe koja vodi Informacioni sistem Univerziteta u Tuzli.

3. Ažurna evidencija svih računarskih i mrežnih resursa

Član 16.
(Administratori sistema)

(1) Administratori sistema odnosno ovlaštene osobe zaduženi su za vođenje ažurne evidencije o računarskim i mrežnim resursima Informacionog sistema Univerziteta.
(2) Svako premještanje računara ili njihovih perifernih uređaja s jedne lokacije na drugu izvodi i evidentira ovlaštena osoba Univerziteta (u daljem tekstu: nadležna služba za poslove informatike).
(3) Zastarjela oprema može se zamijeniti ili staviti van upotrebe samo od strane ovlaštene osobe nadležne službe za poslove informatike.

Član 17.
(Premještanje računara i zamjena zastarjele opreme)

Premještanje računara i zamjenu zastarjele opreme izvodi ovlaštena osoba za poslove informatike.

4. Korisnici Informacionog sistema

Član 18.
(Korisnici Informacionog sistema)

Korisnik Informacionog sistema Univerziteta je svaka osoba koja koristi računarsku opremu, računarske programe i baze podataka, koja razvija programe i aplikacije za podršku poslovnom procesu, koja kreira, organizira i održava baze podataka te koristi računar kao samostalnu radnu stanicu ili kao radnu stanicu na mreži.

Član 19.
(Zabrana mijenjanja konfiguracije)

(1) Korisnici ne smiju mijenjati instaliranu konfiguraciju bilo kojeg sistema informacija što obuhvata njihove radne stanice i prijenosne računare na način koji nije izričito dozvoljen od strane za to ovlaštene osobe.

(2) Korisnici ne smiju mijenjati povezanost na mrežu svojih radnih stanica. Upotreba switch-eva ili drugih uređaja za povezivanje radnih stanica sa vanjskim mrežama, što obuhvata i Internet zahtijeva ovlaštenje od strane za to ovlaštene osobe.

(3) Korisnik Informacionog sistema je odgovoran ako instaliranje ili korištenje bilo kojeg nedozvoljenog softvera prouzrokuje da se sistem zaključa, padne ili da se djelomično ili potpuno izgube podaci.

(4) Korisnici su odgovorni za zaštitu i back-up podataka na svom računaru. Ukoliko je korisniku potrebna stručna pomoć prilikom backup-a podataka može konsultovati administratore Informacionog sistema.

(5) Korisnici ne smiju raditi bilo kakve kopije podataka o poslovanju, a koji se mogu naći pohranjeni na bilo kojem mediju, niti raditi kopije konfiguracijskih i sistemskih datoteka ili softvera u vlašnistvu Univerziteta.

5. Administratori Informacionog sistema (ovlaštene osobe)

Član 20.

(Administrator)

(1) Administrator Informacionog sistema Univerziteta je autorizirani korisnik sa specijalnim ovlaštenjima za rad sa računarom, računarskim programima, bazama podataka, s ovlaštenjima pristupa do računara kao samostalne radne jedinice ili kao jedinice na mreži, a za potrebe administriranja i nadzora nad bazama podataka te administriranja, nadzora i upravljanja računarskom i mrežnom opremom.

(2) Administratoru Informacionog sistema Univerziteta iz člana 20. ovoga Pravilnika Rektor Univerziteta dodjeljuje ovlaštenja za korištenje Informacionog sistema primjereno zahtjevima posla kojeg obavlja.

Član 21.
(Instaliranje novih programa i izmjena postojećih)

(1) Instaliranje novih programa i izmjene postojećih programa smiju obavljati samo za to ovlaštene osobe nadležne službe ili ovlašteni serviseri uz nadzor administratora sistema uz pisani nalog.

(2) Na servere ili lične računare smije se instalirati samo programska podrška za koju je dala saglasnost nadležna osoba za poslove informatike.

(3) Korištenje računarskog hardvera ili softvera koji nije nabavio Univerzitet, dozvoljeno je samo uz saglasnost Rektora.

6. Održavanje sistema od strane vanjskih organizacija

Član 22.

(Održavanje sistema od strane izabranih izvođača)

(1) Održavanje sistema od strane izabranih izvođača radova provodi se uz saglasnost i po uputama zaposlenika koji su za to ovlašteni.

(2) Svaka osoba koja po bilo kojoj osnovi obavlja na Univerzitetu privremene ili povremene poslove održavanja sistema, ili poslove temeljem posebnog ugovora, dužna je pridržavati se odredaba ovoga Pravilnika.

(3) Nadležna osoba za poslove informatike dužna je upoznati osobe iz stava 1. i 2. ovog člana s odredbama ovoga Pravilnika pri davanju odobrenja za korištenje resursa Informacionog sistema Univerziteta.

7. Priključivanje i isključivanje servera i radnih stanica na mrežu

Član 23.
(Zabrana priključivanja i isključivanja)

Korisnicima je zabranjeno priključivanje i isključivanje servera i radnih stanica na lokalnu mrežu bez ovlaštenja nadležne osobe za poslove informatike.

8. Rad na daljinu

Član 24.
(Povezivanje ličnih računara)

Bez prethodnog odobrenja nadležne osobe za poslove informatike korisnicima je zabranjeno:

- povezivanje ličnih računara na Internet ili na neku drugu mrežu ili komunikacijski priključak izvan Informacionog sistema Univerziteta;
- spajanje računara izvan Informacionog sistema Univerziteta na računare i računarske sisteme Univerziteta.

Član 25.
(Obaveza izvještavanja o uočenim nepravilnostima)

O svim uočenim nepravilnostima u radu i korištenju informatičke opreme zaposlenici Unvierziteta dužni su odmah izvijestiti nadležnu osobu za poslove informatike ili osobu odgovornu za provođenje mjera zaštite sigurnosti i provođenje sigurnosne politike.

III. MJERE I SREDSTVA ZAŠTITE SIGURNOSTI

Član 26.
(Prijetnje Informacionom sistemu)

Prijetnje Informacionom sistemu Univerziteta imaju za posljedicu smanjenje resursa, ograničavanje resursa, privremeni prestanak rada Informacionog sistema, gubitak podataka, gubitak programa i podataka ili potpuni gubitak Informacionog sistema.

1. Pristupna prava korisnika

Član 27.
(Prisutpna prava korisnika)

(1) Dodjela pristupnih prava korisnika provodi se s ciljem omogućavanja ispravnog korištenja programa, podataka i resursa Informacionog sistema Univerziteta.
(2) Radi provođenja mjere dodjele pristupnih prava korisnicima mreže, aplikacija i baza podataka Informacionog sistema Univerziteta pohranjenih u računarima, nadležna osoba za poslove informatike dužna je provoditi sljedeće radnje:
   - organizovati i provjeravati autentičnost korisnika koji pristupaju mreži računarskih sistema;
   - organizovati pristup i provesti kontrolu pristupa svim računarskim sistemima univerziteta Finra samo ovlaštenim djelatnicima primjereno zahtjevima posla kojeg obavljaju;
   - omogućiti uređaje i softver za autentifikaciju za korisnike koji imaju velika ovlaštenja pristupa mreži i podacima;
   - provesti sve nadopune, brisanja i promjene u organizaciji i kontroli pristupa računarskim sistemima u skladu s odobrenim zahtjevom krajnjeg korisnika;
   - voditi i održavati ažurnim popis administrativnih pristupnih kodova i lozinki te čuvati taj popis na sigurnom mjestu;
   - onemogućiti anonimni pristup bilo koje vrste do radnih stanica;
   - kontrolisati modemske i slične priključke na mrežu;
   - odobriti instalaciju novih modema.

Član 28.
(Obaveze i odgovornosti korisnika)

(1) Korisnik računarskog sistema je odgovoran za sve računarske transakcije izvršene uz upotrebu njegove korisničke identifikacije i lozinke.
(2) Korisnik Informacionog sistema je dužan poštovati sljedeća pravila:
- zabranjeno je otkrivati lozinke drugima te se lozinka mora odmah promijeniti ako postoji sumnja da je postala poznata drugima;
- zabranjeno je pohranjivati lozinku na mjesto gdje je do nje lako doći;
- lozinka se mora mijenjati u roku ne dužem od 180 dana;
- ne smiju se koristiti lozinke koje se mogu lako pamtiti, lako odgonetnuti ili probiti od strane drugih;
- lozinke moraju sadržavati najmanje sedam znakova i to kombinaciju velikih i malih slova i brojki;
- korisnik mora odjaviti svoj account kada prestaje s radom na računaru duže od 1h;
- radna stanica se mora ugasiti kada nije u upotrebi (npr. preko noći).

(3) Ovlaštena osoba za rad sa ljudsim resursima dužna je odmah obavijestiti nadležnu osobu za poslove informatike o tome da li nekom zaposlenom prestaje radni odnos na Unvierzitetu ili se raspoređuje na drugo radno mjesto, kako bi se mogla promjeniti njegova ovlaštenja za pristup resursima.

2. Zaštitni zid (FIREWALL)

Član 29.
(Zaštitni zid)

(1) Zaštitni zid (FIREWALL) se primjenjuje s ciljem organizacije i kontrole prometa mrežom te sprječavanja nedozvoljenog prometa mrežom.

(2) Radi provođenja mjera organizacije, kontrole i zaštite prometa mrežom nadležna osoba za poslove informatike je dužna:
- primijeniti zaštitni zid za organizaciju i kontrolu prometa podacima između vanjskog svijeta i unutrašnjeg dijela mreže;
- primijeniti zaštitni zid za sprječavanje nedozvoljenog prometa mrežom iznutra prema van;
- primijeniti zaštitni zid za sprječavanje nedozvoljenog prometa mrežom iz vanjskog svijeta prema unutrašnjem dijelu mreže;
- primijeniti zaštitni zid za sprečavanje nedozvoljenog prometa zaštićenim segmentom lokalne mreže od ostale lokalne mreže.

3. Internet i elektronska pošta

Član 30.
(Sigurno korištenje Interneta i elektronske pošte)

(1) Sigurno korištenje Interneta i elektronske pošte provodi se u cilju sprečavanja zaraze računarskim virusom, slučajnog gubitka programa i/ili podataka, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenog korištenja resursa, sprečavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.

(2) Univerzitet smatra Internet usluge kao sredstvo koje može značajno da poveća produktivnost. Zbog toga, korisnici imaju mogućnost da ga koriste zbog poslovnih interesa Unvierziteta.

(3) Nadležna osoba za poslove informatike obezbjeđuje opremu i parametre potrebne za pristup Internet uslugama. Strogo se zabranjuje modifikacija parametara na načine koji nisu odobreni od strane nadležne osobe za poslove informatike

(4) Usluge Interneta a posebno World Wide Web (WWW) predstavljaju važne izvore informacija za Univerzitet. Iz razloga što ne postoji kontrola kvaliteta informacija koje su dostupne preko Interneta, informacije koje se preuzmu sa Interneta treba uvijek pažljivo koristiti.

(5) Korisnicima nije dozvoljeno da preuzimaju softver sa Interneta u privatne svrhe.

(6) Korisnicima nije dozvoljen pristup Internetu sa sistema računara koji sadrži stratešku informaciju čak i kada je nadležna osoba za poslove informatike poduzela sve moguće mjere zaštite.

(7) Radi sigurnog korištenja Interneta i elektronske pošte potrebno je provoditi sljedeće radnje:
- dozvoljen je svaki oblik komunikacije putem Interneta (ZOOM, društvene mreže,Forumi, Skype, Viber i sl.) koja se obavlja iz profesionalnih razloga i koja ne utječe negativno na produktivnost;
- dozvoljeno je korištenje web explorera za prikupljanje poslovnih informacija s komercijalnih web adresa;
- dozvoljeno je korištenje Interneta za pristup bazama podataka radi pronalaženja poslovnih informacija;
- nadležna osoba za poslove informatike obezbjeđuje alat potreban za rad e- mail usluga. Strogo je zabranjena modifikacija ovih alata i korištenje alata koje nije nabavio Univerzitet;
- poruke koje obrađuje e-mail sistem univerziteta Finra predstavljaju vlasništvo Univerziteta;
- korisnicima nije dozvoljen pristup računima koji nisu njima dodijeljeni ili da koriste e-mail sistem pod identitetom drugih korisnika;
- dozvoljeno je korištenje elektronske pošte u svrhu ostvarivanja poslovnih kontakata;
- za poslovnu komunikaciju obavezno je korištenje zvanične e-mail adrese koju korisniku dodjeljuje administrator Informacionog sistema;
- korisnik Interneta i elektronske pošte snosi odgovornost za sadržaj svih tekstova, zvučnih zapisa ili slika koje objavljuje ili šalje putem Interneta;
- uz svaku komunikaciju putem Interneta mora biti naznačeno ime zaposlenog koji je obavlja;
- zabranjeno je slanje i prosljeđivanje lančane elektronske pošte, tj. poruka koje uključuju procedure za prosljeđivanje poruka drugima;
- zabranjeno je slanje iste poruke na više od deset (10) prijemnih adresa ili na više od jedne dostavne (distribucijske) liste, osim u slučajevima kada to priroda komunikacije zahtijeva;
- kada se korisniku dodjeljuje e-mail adresa potrebno je slijediti slijedeća uputstva: - E-mail adresa treba da sadrži:*ime.prezime@finra.ba*;
- s vremena na vrijeme korisnici treba da izbrišu iz sistema poruke i priloge koji nisu od važnosti za poslove univerziteta Finra. E-mail poruke koje su relevantne za poslove Univerziteta i koje se moraju duže vremena čuvati treba spasiti izvan e-mail sistema u fajling sistem ili bazu podataka koju podržava adekvatan back-up sistem;
- ako korisnik primi poruku koja se ne odnosi na njega treba da obavijesti administratore Informacionog sistema i poduzme mjere da zaštiti tajnost poruke;
- korisnici ne smiju odgovarati na nepoznate e-mail poruke. Korisnici treba da imaju na umu da porijeklo e-mail poruke može biti falsifikovano ili adresa pošiljaoca korištena bez dozvole stvarnog vlasnika;
- zabranjeno je obavljanje privatnih i osobnih poslova uz korištenje resursa Informacionog sistema Univerziteta;
- zabranjeno je slanje bilo kakvog sadržaja koji je ofanzivan, koji primatelju može stvoriti neprilike ili štetu, ili je obmanjujući;
- antivirusna zaštita mora biti obavezno aktivirana kod prijema elektronske pošte i pridruženih datoteka;
- zabranjeno je pokretanje izvršnih datoteka ako se ne zna o čemu se radi i da li je izvor pouzdan. Korisnik treba da je svjestan opasnosti od virusa u korištenju e-mail sistema. Korisnici naročito treba da imaju na umu da prilozi uz e-mail mogu da sadrže viruse iako izgleda da je poruku poslao pouzdan korisnik;
- Zbog ograničenja u infrastrukturi komunikacija, nadležna služba za poslove informatike može da uvede ograničenje na dužinu korisnikovih e-mail poruka (odlazećih i dolazećih) kao i veličinu prostora određenog za pohranjivanje poruka;
- Politika Univerziteta je da obezbijedi tehnička sredstva za povećanje stepena tajnosti, integriteta i dostupnosti e-mail usluga. Međutim, korisnici treba da imaju na umu da se ne može garantovati sigurnost e-mail poruka pogotovu kada e-mail porukama rukuju e-mail sistemi koji nisu pod direktnom kontrolom Univerziteta ;
- osim ako se ne koriste odgovarajuće kriptografske tehnike, korisnici treba da izbjegavaju korištenje e-mail sistema za slanje osjetljivih informacija kao što su brojevi kreditnih kartica, lični podaci i informacije koje su označene kao *Ograničene* ili *Povjerljive;*
- osim ako se ne koriste tehnike potvrde vjerodostojnosti i integriteta korisnici treba da znaju da e-mail sistem ne može garantovati da je primljene poruke poslao dotični pošiljalac te da nisu usput bile izmijenjene,
- korisnici ne treba da šalju poruke na način koji se protivi propisima o zaštiti ličnih podataka ili drugim propisima u pogledu tajnosti podataka.

(8) U slučaju zloupotrebe korištenja interneta i elektronske pošte od strane korisnika IS-a univerziteta Finra, a na zahtjev rukovodioca nadležne službe, administrator Informacionog sistema može ograničiti ili onemogućiti upotrebu interneta i elektronske pošte.

(9) Upotrebljivost sigurnosne kopije podataka provjerava se najmanje svakih šest mjeseci, uz provjeru postupka povraćaja baza podataka uskladištenih na mediju, tako da vraćeni podaci nakon izvršene provjere budu cjeloviti, povjerljivi i dostupni za korištenje.

(10) Puna zaštita (backup) za sve serverske mašine radi se obavezno jednom godišnje software-om za full-backup serverskih mašina, a po potrebi i češće (ukoliko je bilo izmjena u operativnom sistemu, dodavanja novih patch-eva, file-system-a i slično).

Član 31.
(Oznake)

(1) Svaki medij mora imati oznaku na kojoj su navedeni podaci o sadržaju. Za izvorne programe mora biti navedeno: tačan naziv aplikacije i datum.
(2) Svaki uređaj na kojima se štite podaci mora imati oznaku sa slijedećim podacima:
- aplikacija, odnosno grupa poslova;
- datum zaštite.

(3) Za ostale korisnike, koji posao obavljaju na personalnom računaru, propisuje se isti način zaštite podataka na optičkim ili magnetnim medijima. Korisnici su sami dužni napraviti i čuvati ovu zaštitu u slučaju da hardwerski strada disk i na taj način im propadnu podaci (razne vrste korisničkih izvještaja).
(4) Po isteku roka čuvanja podataka na medijima potrebno je nepovratno izbrisati sadržaj medija.

Član 32.

(Obezbjeđenje pristupa)

Nadležna osoba za poslove informatike dužna je obezbijediti pristup „CLOUD“ servisima ili mrežnim uređajima za potrebe backup-a baza podataka IS-a i dokumenata od važnosti za poslovanje Univerziteta.

4. Fizička zaštita prostorija s opremom

Član 33.
(Fizička zaštita prostorija)

(1) Fizička zaštita prostorija s opremom provodi se u cilju sprečavanja kvara opreme, krađe opreme, prekida ili neurednog napajanja električnom energijom, požara ili elementarnih nepogoda, krađe programa i/ili podataka, neovlaštenog pristupa i korištenja podataka i/ili programa, neovlaštenog korištenja resursa, sprečavanja drugih u korištenju resursa te namjernog uništenja opreme i/ili programa i/ili podataka.
(2) Radi provođenja fizičke zaštite prostorija s opremom potrebno je provoditi sljedeće radnje:
- serveri i aktivna mrežna oprema se moraju smjestiti u sigurnim i čvrstim zgradama koje nisu izložene poplavi;
- serveri i mrežna oprema se moraju štititi stalnim izvorom energije (UPS), a ostala računarska oprema štiti se od strujnih udara stabilizatorima napona;
- prostorije sa serverima se moraju štititi od visoke ili niske vlažnosti zraka te ekstremne topline ili hladnoće klimatizacijskim uređajima;
- prostorije s računarskom opremom moraju biti zaštićene od požara u skladu sa Pravilnikom o zaštiti od požara;
- prostorija s glavnim komunikacijskim čvorom i telefonskom centralom mora biti zaključana i pristup dozvoljen samo uz prisustvo ovlaštene osobe;
- u trenucima kada nitko ne boravi u prostorijama s računarskom opremom, vrata moraju biti zaključavana, a prozori zatvarani;
- u slučaju krađe ili gubitka ključa od prostorije s računarskom opremom treba obavijestiti odgovornu osobu i zamijeniti bravu;
- na sva vanjska vrata i prozore moraju biti instalirani uređaji za dojavu nasilnog ulaza i moraju se redovito kontrolisati;
- oprema koja mora biti smještena na javno pristupnom prostoru mora biti zaštićena, a javni pristup nadziran;

- na ulazu u zgradu moraju se pratiti kretanje svih osoba na ulazu;
- nepoznate osobe moraju pružiti dokaze o svojem identitetu;
- pristup do uređaja za obradu podataka mora biti kontroliran i dozvoljen samo ovlaštenim osobama;
- područje na kojem se obavlja isporuka i preuzimanje opreme ili potrošnog materijala mora biti kontrolirano i po mogućnosti odvojeno od područja gdje se nalaze sredstva za obradu podataka.

IV. PROVOĐENJE MJERA I SREDSTAVA ZAŠTITE SIGURNOSTI

1. Načini provođenja

Član 34.
(Provođenje propisanih mjesra i sredstava zaštite sigurnosti)

(1) Poduzimanje i provođenje propisanih mjera i sredstava zaštite sigurnosti Informacionog sistema Univerziteta provodi se u skladu s odredbama ovoga Pravilnika.

(2) Nadležna osoba za poslove informatike neposredno organizira i nadzire provođenje mjera i sredstava zaštite sigurnosti utvrđenih ovim Pravilnikom.

(3) U cilju unapređenja zaštite sigurnosti Informacionog sistema odgovorna osoba za provođenje mjera i sredstava zaštite sigurnosti predlaže, osim mjera i sredstava utvrđenih ovim Pravilnikom, provođenje drugih mjera zaštite sigurnosti u skladu sa zakonom i opće prihvaćenim pravilima struke.

(4) Odgovorna osoba za provođenje mjera i sredstava zaštite sigurnosti pri obavljanju kontrole i nadzora nad provođenjem mjera zaštite sigurnosti dužna je izvijestiti neposrednog rukovodioca kod kojeg je nadzor obavljen o rezultatima kontrole i unijeti ih u redovne izvještaje.

(5) Ako odgovorna osoba za provođenje mjera zaštite sigurnosti pristupa rješavanju složenijih problema s područja zaštite sigurnosti Informacionog sistema sarađivat će sa svim zaposlenicima Unvierziteta.

Član 35.
(Poslovi odgovorne osobe)

(1) Odgovorna osoba za provođenje mjera zaštite sigurnosti obavlja sljedeće poslove:
- obavlja redovnu kontrolu provođenje mjera zaštite sigurnosti utvrđenih ovim Pravilnikom;
- sarađuje i koordinira rad na izradi uputa za zaštitu sigurnosti Informacionog sistema;
- vodi brigu o pravovremenom osposobljavanju zaposlenih za zaštitu sigurnosti Informacionog sistema, te vodi brigu o tome,
- izvještava Rektora Univerziteta o utvrđenim nepravilnostima u pogledu sigurnosnih uvjeta i predlaže mjere za otklanjanje istih.

(2) Prilikom obavljanja kontrole provođenja mjera zaštite sigurnosti Informacionog sistema Unvierziteta propisanih ovim Pravilnikom, odgovorna osoba ima sljedeća ovlaštenja:
- narediti prekid obavljanja posla ili radnje kojom se neposredno ugrožava sigurnost Informacionog sistema, te o tome obavjestiti Rektora Univerziteta,
- izvijestiti Rektora o neprovođenju propisanih mjera zaštite sigurnosti.

2. Subjekti provođenja

Član 36.
(Provođenje mjera)

Svaki zaposleni na Unvierzitetu dužan je poduzimati i provoditi propisane mjere i sredstva zaštite sigurnosti Informacionog sistema Univerziteta u skladu s ovim Pravilnikom.

Član 37.
(Novi zaposlenik)

Novi zaposlenik na Univerzitetu dužan je:

- upoznati se s odredbama ovog Pravilnika prije stupanja na rad i samostalnog obavljanja poslova na radnom mjestu, kao i svladati osposobljavanje za provođenje mjera zaštite sigurnosti;
- poduzimati i provoditi propisane mjere zaštite sigurnosti na radnom mjestu i u radnom prostoru;
- svaku uočenu opasnost koja bi mogla biti prijetnja ugrožavanju sigurnosti sistema odmah prijaviti neposrednom rukovodiocu ili osobi odgovornoj za provođenje mjera zaštite sigurnosti.

3. Edukacija korisnika i administratora

Član 38.
(Osposobljavanje zaposlenika)

(1) Odgovorna osoba za provođenje mjera i sredstava zaštite sigurnosti dužna je osigurati osposobljavanje zaposlenika Univerziteta za provođenje mjera i sredstava zaštite propisanih ovim Pravilnikom.
(2) Obaveza iz stava 1 ovoga člana odnosi se i na djelatnike koji su zaposleni na određeno vrijeme.

4. Korisnički i administratorski priručnici

Član 39.
(Korisnički i administratorski priručnici)

(1) Odgovorna osoba za provođenje mjera i sredstava zaštite sigurnosti dužna je osigurati korisničke i administratorske priručnike.
(2) Korisnički i administratorski priručnici sadrže upute za korisnike i administratore Informacionog sistema za korištenje resursa Informacionog sistema Univerziteta u skladu s odredbama ovoga Pravilnika.

5. Postupanje u incidentnim situacijama

Član 40.
(Postupanje u incidentnim situacijama)

(1) U slučaju havarije ili incidentne situacije djelatnik Univerziteta je dužan odmah obavjestiti odgovornu osobu za provođenje mjera zaštite sigurnosti.
(2) Pod havarijom u smislu ovoga Pravilnika smatra se:
    - potpuni gubitak sistema;
    - gubitak programa;
    - gubitak podataka.
(3) Pod incidentnim situacijama u smislu ovoga Pravilnika smatraju se:
    - privremeni prestanak rada sistema;
    - gubitak opreme;
    - ograničavanje resursa u radu;
    - smanjenje resursa;
    - kvar opreme;
    - sve drugo što može ugroziti Informacioni sistem Univerziteta.

6. Nadzor

Član 41.
(Nadzor nad primjenom mjera i sredstava zaštite sigurnosti)

(1) Nadzor nad primjenom mjera i sredstava zaštite sigurnosti Informacionog sistema Univerziteta obavlja se sukladno odredbama ovoga Pravilnika.
(2) Nadzor nad primjenom mjera i sredstava zaštite sigurnosti organizira i provodi odgovorna osoba za provođenje mjera i sredstava zaštite sigurnosti.

7. Stalni i povremeni nadzor

Član 42.
(Stalni i povremeni nadzor)

Nadležna osoba za poslove informatike za provedbu mjera i sredstava zaštite sigurnosti dužna je provoditi stalni i povremeni nadzor provedbe mjera i sredstava zaštite propisanih ovim Pravilnikom.

V. ODGOVORNOST ZBOG NEPRIDRŽAVANJA MJERA I SREDSTAVA ZAŠTITE SIGURNOSTI

Član 43.

(Odgovorna osoba za provođenje mjera zaštite sigurnosti i sigurnosne politike)

(1) Osoba odgovorna za provođenje mjera zaštite sigurnosti i provođenje sigurnosne politike u skladu s ovim Pravilnikom je nadležna osoba za poslove informatike Univerziteta.

(2) Odgovorna osoba za provođenje mjera zaštite sigurnosti redovno obavlja kontrolu provođenja mjera zaštite utvrđenih ovim Pravilnikom i odgovorna je za provođenje tih mjera.

Član 44.
(Pridržavanje mjera i sredstava zaštite)

(1) Korisnik Informacionog sistema Univerziteta je dužan pridržavati se svih mjera i sredstava zaštite propisanih ovim Pravilnikom.

(2) Ako korisnik nepridržavanjem odredaba ovoga Pravilnika nanese štetu Unvierzitetu, odgovara za pričinjenu štetu.

VI. ZAVRŠNE ODREDBE

Član 45.

(Izjava o prihvatanju sigurnosne politike)

Svaki korisnik Informacionog sistema Univerziteta dužan je potpisati Izjavu o prihvatanju sigurnosne politike Informacionog sistema Univerziteta (Prilog 1).

Član 46.
(Skup pravila)

Rektor Univerziteta donijet će u roku od jedne godine dana od dana stupanja na snagu ovoga Pravilnika skup pravila, i to:

- Plan oporavka u slučaju havarije;
- Plan zaštite i povrata podataka;
- Plan provođenja antivirusne zaštite;
- Plan postupanja u incidentnim situacijama;
- Oblici saradnje administratora s korisnikom.

Član 47.

(Izmjene i dopune Pravilnika)

(1) Ovaj Pravilnik se može mijenjati i dopunjavati u zavisnosti od vlastititih potreba i/ili zbog obaveza nametnutih propisima viših organa.

(2) Prijedlog za promjene pravilnika zbog razloga navedenih u prethodnom stavu, podnosi ovlaštena osoba, a podnosi ga Rektoru Unvierziteta.

Član 48.
(Postupanje suprotno odredbama Pravilnika)

Svako postupanje koje je suprotno odredbama ovog Pravilnika smatra se zloupotrebom i prekoračenjem službenih ovlaštenja i podliježe disciplinskoj odgovornosti.

Član 49.
(Stupanje na snagu)

Pravilnik stupa na snagu danom donošenja, od kada se i primjenjuje.

Broj: 03-1176-5-18/24
Tuzla, 26.12.2024. godine

PREDSJEDAVAJUĆI SENATA

VISOKOŠKOLSKA USTANOVA UNIVERZITET
UNIVERZITET FINRA
Univerzitet FINRA
Prof. dr. sc. Ismet Kalić, *v.d. rektor*

Prilog 1.

I Z J A V A
O PRIHVATANJU SIGURNOSNE POLITIKE Informacionog sistema UNIVERZITETA FINRA Tuzla

Potpisivanjem ove Izjave izjavljujem da sam:

1. Primio i pročitao Pravilnik o sigurnosti Integralnog Informacionog sistema Univerziteta FINRA Tuzla i razumio ga.

2. Razumio sam i slažem se da svaki računar, softver i memorijski medij koji mi je nabavio Univerzitet FINRA Tuzla sadrži vlasništvom zaštićene i povjerljive informacije o univerzitetu Finra i njenim poslovnim partnerima te da one jesu i ostaju vlasništvo Univerziteta FINRA Tuzla u svim svojim dijelovima i trajno.

3. Slažem se da neću kopirati, umnožavati (s izuzetkom sigurnosnog kopiranja kao dijela mojih radnih obaveza na Univerzitetu FINRA Tuzla), na bilo koji način objavljivati i omogućiti bilo kome drugome da kopira bilo koji dio tih informacija ili softvera.

4. Slažem se da ću, prestankom radnog odnosa na Univerzitetu FINRA Tuzla iz bilo kojeg razloga, odmah vratiti izvorni primjerak i sve kopije svog softvera, računarskog materijala i računarske opreme koje sam primio od Univerziteta FINRA Tuzla, a koji su u mome posjedu ili na bilo koji drugi način pod mojom kontrolom.

Ime i prezime zaposlenika:

Fakultet:

Datum:

Potpis zaposlenika
