Visokoškolska ustanova
Univerzitet FINRA Tuzla

Procedura zaštite podataka i sigurnosti informacionog sistema

Decembar, 2025. godine

Na osnovu člana 63. Zakona o visokom obrazovanju Tuzlanskog kantona – prečišćeni tekst („Službene novine Tuzlanskog kantona“, broj: 21/21, 22/21, 5/22, 11/22, 16/22 i 5/25), i člana 39. Statuta Univerziteta, na 22. (dvadesetdrugoj) sjednici održanoj dana 29.12.2025. godine, Senat visokoškolske ustanove Univerzitet FINRA Tuzla donosi:

PROCEDURU
zaštite podataka i sigurnosti informacionog sistema

Član 1.
(Predmet)

Procedurom zaštite podataka i sigurnosti informacionog sistema utvrđuju se mjere, pravila i procedure zaštite podataka i sigurnosti informacionog sistema Univerziteta, u cilju očuvanja integriteta, povjerljivosti i dostupnosti podataka i informacionih resursa Univerziteta.

Član 2.
(Ciljevi)

Cilj je da se Procedurom zaštite podataka i sigurnosti informacionog sistema (u daljem tekstu: Procedura) osigura povjerljivost, integritet i dostupnost svih podataka, spriječi neovlašteni pristup, gubitak ili zloupotrba podataka, definišu odgovornosti svih uposlenika i studenata u zaštiti podataka, te da se obezbijedi kontinuitet rada informacionog Sistema Univerziteta.

Član 3.
(Obuhvat)

Procedura se odnosi na: sve informacione sisteme i baze podataka Univerziteta, računarsku mrežu, servere, cloud servise i sigurnosne aplikacije, lične podatke zaposlenika, studenata i vanjskih saradnika, dokumentaciju i komunikacione kanale (e-mail, e-UIS, LMS, aplikacije).

Član 4.
(Definicije)

Definicije pojmova koji se koriste u ovoj procedure, imaju značenja kako slijedi:
a) Podaci – sve informacije koje se čuvaju, obrađuju ili prenose putem informacionog sistema.
b) Informacioni sistem – skup hardverskih, softverskih i mrežnih komponenti Univerziteta FINRA Tuzla.
c) Administrator sistema – osoba zadužena za održavanje i sigurnost sistema.
d) Korisnik – svaka osoba (zaposlenik, student, saradnik) koja koristi resurse Univerziteta.

Član 5.
(Načela zaštite podataka)

Načela na kojima se zasniva primjena procedure su:

1. Zakonitost i poštena obrada podataka;
2. Transparentnost u prikupljanju i obradi podataka;
3. Minimalizacija podataka – prikupljaju se samo nužni podaci;
4. Tačnost i redovno ažuriranje podataka;
5. Sigurnost kroz tehničke i organizacione mjere;
6. Ograničeno čuvanje podataka – u skladu s propisanim rokovima.

Član 6.
(Mjere tehničke zaštite)

Mjere tehničke zaštite koje se poduzimaju s ciljem zaštite podataka i sigurnosti informacionog sistema su:

- Korištenje jakih lozinki i dvostruke autentifikacije;
- Redovno ažuriranje softvera i antivirusne zaštite;
- Enkripcija podataka u prijenosu i pohrani;
- Backup podataka na dnevnom i mjesečnom nivou;
- Segmentacija mreže i firewall zaštita;
- Kontrola pristupa podacima prema principu „potrebe za znanjem“.

Član 7.
(Mjere organizacione zaštite)

Mjere organizacione zaštite koje se poduzimaju s ciljem zaštite podataka i sigurnosti informacionog sistema su:

- Ograničavanje pristupa podacima na osnovu radnog mjesta i odgovornosti;
- Potpisivanje Izjave o povjerljivosti od strane zaposlenika i saradnika;
- Obavezna edukacija zaposlenika o kibernetičkoj sigurnosti;
- Incident Response procedura za prijavu sigurnosnih incidenata;
- Revizija i monitoring sistema najmanje jednom godišnje.

Član 8.
(Odgovornosti)

(1) Predsjednik uprave i rektor Univerziteta odgovorni su za primjenu pravila Procedure, kao i za praćenje da se propisane mjere zaštite podataka i sigurnosti informacionog sistema sprovode u skladu sa utvrđenim pravilima.

(2) Radnici zaposleni u Službi informacionih tehnologija koordiniraju implementaciju Procedure, te primjenjuju tehničke mjere zaštite.

(3) Radnici Univerziteta su dužni koristiti informacioni sistem u skladu s pravilima ove Procedure.

Član 9.
(Postupak u slučaju incidenta)

(1) Svaki radnik koji koristi informacioni sistem dužan je odmah prijaviti sigurnosni incident administratoru sistema, predsjedniku uprave i rektoru Univerziteta.
(2) Nakon prijave incidenta, administrator sistema kroz vrši analizu prijavljenog incidenta i dokumentuje incident sa svim relevantnim podacima o nastanku incidenta, eventualnoj šteti koja je nastala incidentom, te podatke o saniranju nastale štete. Administrator sistema ove aktivnosti dokumentuje u pismenoj formi izvještaja o incidentu, kojeg dostavlja predsjedniku uprave, rektoru i senatu.
(3) Ako incident uključuje povredu ličnih podataka, obavještava se Agencija za zaštitu ličnih podataka BiH.

Član 10.
(Praćenje i revizija)

Procedura se revidira svake dvije godine ili ranije, ukoliko to zahtijevaju zakonske izmjene ili promjene u informacionom sistemu.

Član 11.
(Tumačenje)

Nadzor nad provedbom ove Procedure vrši predsjednik uprave, rektor Univerziteta i dekani fakulteta, a tumačenje Procedure vrši Senat Univerziteta.

Član 12.
(Stupanje na snagu i primjena)

Procedura stupa na snagu danom donošenja, od kada se i primjenuje.

Broj: 02-xxxx/25
Tuzla, 29.12.2025. godine

PREDSJEDAVAJUĆI SENATA

_____

/ prof.dr.sc. Hadžib Salkić, rektor/