

**VISOKA ŠKOLA eMPIRICA  
BRČKO DISTRIKT BiH**

**P R A V I L N I K**  
**O ZAŠTITI LIČNIH PODATAKA  
I INFORMACIONOJ SIGURNOSTI  
VISOKE ŠKOLE eMPIRICA BRČKO DISTRIKT BiH**



**Brčko, juli 2026. godine**

Na osnovu Zakona o zaštiti ličnih podataka („Službeni glasnik Bosne i Hercegovine“, broj 12/25), Zakona o visokom obrazovanju u Brčko distriktu Bosne i Hercegovine („Službeni glasnik Brčko distrikta BiH“, broj 21/24 – prečišćeni tekst i 4/26), Statuta i drugih opštih akata Visoke škole eMPIRICA Brčko distrikt BiH, Senat Visoke škole eMPIRICA Brčko distrikt BiH, na sjednici održanoj u julu 2026. godine, donosi

**P R A V I L N I K**  
**O ZAŠTITI LIČNIH PODATAKA**  
**I INFORMACIONOJ SIGURNOSTI**  
**VISOKE ŠKOLE eMPIRICA BRČKO DISTRIKT BiH**

**I OSNOVNE ODREDBE**

**Član 1.**

*(Predmet Pravilnika)*

- (1) Ovim pravilnikom uređuju se načela, odgovornosti, prava, organizacione i tehničke mjere za zakonitu obradu ličnih podataka i zaštitu povjerljivosti, cjelovitosti i dostupnosti informacija Visoke škole eMPIRICA Brčko distrikt BiH.

**Član 2.**

*(Cilj)*

- (1) Cilj je zaštita prava i sloboda fizičkih lica, akademskih i poslovnih podataka i kontinuiteta rada, uz omogućavanje zakonitog obrazovanja, istraživanja i upravljanja ustanovom.

**Član 3.**

*(Obuhvat)*

- (1) Pravilnik se primjenjuje na papirne i elektronske podatke, sisteme, uređaje, mreže, usluge u oblaku, komunikaciju, video i audio zapise, rezervne kopije i podatke koje u ime Visoke škole obrađuje drugo lice.
- (2) Primjenjuje se na zaposlene, angažovana lica, studente, dobavljače i druga lica kojima je odobren pristup.

**Član 4.**

*(Značenje izraza)*

- (1) Visoka škola je kontrolor kada određuje svrhu i način obrade ličnih podataka.
- (2) Lični podatak je svaki podatak koji se odnosi na identifikovano ili odredljivo fizičko lice, a obrada je svaka radnja sa takvim podatkom.
- (3) Informaciona sigurnost je očuvanje povjerljivosti, cjelovitosti, dostupnosti, autentičnosti i sljedivosti informacija.
- (4) Incident je događaj koji ugrožava ili može ugroziti podatke, sistem, uslugu ili prava lica.

**Član 5.**

*(Načela obrade)*

- (1) Lični podaci obrađuju se zakonito, pravično i transparentno, za određenu svrhu, u najmanjem potrebnom obimu, tačno, uz ograničen rok čuvanja i odgovarajuću sigurnost.

- (2) Visoka škola mora moći dokazati usklađenost sa ovim načelima.

#### **Član 6.**

*(Načelo razmjernosti)*

- (1) Mjera nadzora, provjere identiteta ili sigurnosti mora biti primjerena riziku i ne smije zadirati u privatnost više nego što je nužno za zakonitu svrhu.

#### **Član 7.**

*(Rodna ravnopravnost izraza)*

- (1) Izrazi upotrijebljeni u jednom gramatičkom rodu odnose se bez diskriminacije na sva lica.

## **II UPRAVLJANJE I ODGOVORNOSTI**

#### **Član 8.**

*(Odgovornost Visoke škole)*

- (1) Visoka škola utvrđuje svrhe, pravne osnove, kategorije podataka i lica, rokove, primaoce, mjere zaštite i način ostvarivanja prava.

#### **Član 9.**

*(Odgovornost direktora)*

- (1) Direktor obezbjeđuje resurse, razdvajanje odgovornosti, upravljanje rizicima, ugovore sa obrađivačima, reagovanje na incidente i izvršenje preporuka nadležnog organa.

#### **Član 10.**

*(Službenik za zaštitu podataka)*

- (1) Kada je imenovanje obavezno ili opravdano obimom i rizikom obrade, Visoka škola imenuje službenika za zaštitu podataka sa nezavisnim pristupom rukovodstvu i bez sukoba interesa.
- (2) Službenik savjetuje, prati usklađenost, učestvuje u procjeni uticaja, sarađuje sa Agencijom i predstavlja kontakt za lica, ali ne preuzima odgovornost kontrolora.

#### **Član 11.**

*(Odgovorno lice za informacionu sigurnost)*

- (1) Direktor određuje lice ili funkciju koja koordinira tehničke mjere, upravljanje pristupom, ranjivostima, rezervnim kopijama, kontinuitetom i incidentima.

#### **Član 12.**

*(Vlasnik informacije ili procesa)*

- (1) Za ključnu zbirku ili proces određuje se odgovorno lice koje klasifikuje podatke, odobrava pristup, utvrđuje rok čuvanja i periodično provjerava opravdanost obrade.

#### **Član 13.**

*(Obaveze korisnika)*

- (1) Korisnik pristupa samo podacima potrebnim za ulogu, čuva pristupne podatke, koristi odobrenu opremu i kanale, poštuje povjerljivost i odmah prijavljuje incident ili sumnju.

#### **Član 14.**

*(Obrađivači i dobavljači)*

- (1) Lice koje obrađuje podatke u ime Visoke škole bira se nakon procjene sposobnosti da obezbijedi zakonitost i sigurnost i angažuje pisanim ugovorom sa propisanim obavezama.
- (2) Podobrađivač se angažuje samo uz prethodno odobrenje i iste zaštitne obaveze.

#### **Član 15.**

*(Povjerljivost)*

- (1) Lice sa pristupom obavezuje se na povjerljivost koja traje i nakon prestanka radnog, studijskog ili ugovornog odnosa.

### **III ZAKONITOST, TRANSPARENTNOST I EVIDENCIJE OBRADE**

#### **Član 16.**

*(Pravni osnov)*

- (1) Prije obrade utvrđuje se odgovarajući pravni osnov: zakonska obaveza, izvršenje ugovora, javni ili legitimni interes kada je dopušten, zaštita životno važnog interesa, saglasnost ili drugi osnov propisan zakonom.
- (2) Saglasnost se ne koristi kada lice nema stvaran i slobodan izbor ili kada postoji primjereniji pravni osnov.

#### **Član 17.**

*(Određivanje svrhe)*

- (1) Svrha se određuje prije prikupljanja i mora biti konkretna i razumljiva; nova nespojiva svrha zahtijeva novu procjenu i odgovarajući osnov.

#### **Član 18.**

*(Smanjenje obima podataka)*

- (1) Prikupljaju se samo podaci nužni za svrhu, a obrazac, sistem i izvještaj periodično se provjeravaju radi uklanjanja suvišnih polja i kopija.

#### **Član 19.**

*(Tačnost)*

- (1) Organizaciona jedinica obezbjeđuje razuman način provjere, ažuriranja i ispravke podataka, naročito prije donošenja odluke koja utiče na pravo lica.

#### **Član 20.**

*(Posebne kategorije podataka)*

- (1) Podaci o zdravlju, biometriji, vjeri, političkom mišljenju, sindikalnom članstvu i druge posebne kategorije obrađuju se samo kada postoji poseban zakonski uslov i pojačane mjere zaštite.

#### **Član 21.**

*(Podaci o krivičnim osudama i postupcima)*

- (1) Ovi podaci obrađuju se samo pod kontrolom nadležnog organa ili kada je obrada izričito dopuštena zakonom, uz strogo ograničen pristup i rok.

## **Član 22.**

*(Podaci djece i maloljetnih lica)*

- (1) Kada obrada uključuje dijete ili maloljetno lice, informacije se daju jasnim jezikom, procjenjuje se najbolji interes djeteta i pribavlja saglasnost nosioca roditeljske odgovornosti kada je zakonom potrebna.

## **Član 23.**

*(Obavještenje o privatnosti)*

- (1) Pri prikupljanju se licu daju podaci o kontroloru, svrsi i osnovu, primaocima, roku, pravima, kontaktu, prenosu i eventualnom automatizovanom odlučivanju, osim kada zakon dopušta izuzetak.
- (2) Obavještenje mora biti lako dostupno, slojevito kada je opširno i prilagođeno kanalu prikupljanja.

## **Član 24.**

*(Saglasnost)*

- (1) Saglasnost mora biti dokaziva, posebna, informisana i nedvosmislena i može se povući jednako jednostavno kao što je data, bez uticaja na ranije zakonitu obradu.

## **Član 25.**

*(Evidencija aktivnosti obrade)*

- (1) Visoka škola vodi i ažurira evidenciju aktivnosti obrade sa svrhama, kategorijama lica i podataka, primaocima, prenosima, rokovima i opštim opisom mjera sigurnosti.

## **Član 26.**

*(Zaštita podataka po dizajnu i po pravilu)*

- (1) Novi proces, sistem, obrazac ili usluga projektuje se sa najmanjim potrebnim obimom podataka, ograničenim pristupom, sigurnim početnim postavkama i određenim rokom čuvanja.

## **Član 27.**

*(Procjena uticaja)*

- (1) Prije obrade koja vjerovatno stvara visok rizik, naročito kod sistematskog nadzora, biometrije, osjetljivih podataka ili novih tehnologija, provodi se procjena uticaja na zaštitu podataka.
- (2) Ako se visok rizik ne može ublažiti, postupa se prema obavezi prethodnog savjetovanja sa nadležnom Agencijom.

## **Član 28.**

*(Istraživanje i statistika)*

- (1) Podaci za istraživanje i statistiku koriste se uz odobrenje, etičku i pravnu procjenu, smanjenje obima, pseudonimizaciju ili anonimizaciju kada je moguća i zabranu pokušaja ponovne identifikacije.

#### **Član 29.**

*(Video, audio i snimanje nastave)*

- (1) Snimanje se dopušta samo uz određenu svrhu, pravni osnov, prethodno obavještenje, ograničen pristup i rok brisanja.
- (2) Skriveno ili trajno snimanje prostora, sastanaka ili nastave nije dopušteno bez izričitog zakonskog osnova i procjene nužnosti.

#### **Član 30.**

*(Automatizovano odlučivanje)*

- (1) Odluka sa pravnim ili sličnim značajnim učinkom ne zasniva se isključivo na automatizovanoj obradi, osim kada je to dopušteno zakonom i praćeno zaštitnim mjerama, uključujući ljudsku intervenciju i mogućnost osporavanja.

### **IV PRAVA LICA**

#### **Član 31.**

*(Način ostvarivanja prava)*

- (1) Zahtjev se može podnijeti elektronski ili pisano kroz objavljeni kanal, uz provjeru identiteta koja je razmjerna riziku.
- (2) Odgovor se daje bez nepotrebnog odlaganja i u zakonskom roku, jasno i u pravilu bez naknade.

#### **Član 32.**

*(Pravo na pristup)*

- (1) Lice ima pravo na potvrdu da li se njegovi podaci obrađuju, kopiju podataka i informacije o svrsi, kategorijama, primaocima, roku, izvoru, pravima i automatizovanom odlučivanju.
- (2) Pristup ne smije neopravdano ugroziti prava i povjerljive podatke drugog lica.

#### **Član 33.**

*(Pravo na ispravku)*

- (1) Netačan podatak ispravlja se, a nepotpun dopunjava uzimajući u obzir svrhu obrade; o ispravci se obavještavaju primaoci kada to zakon zahtijeva.

#### **Član 34.**

*(Brisanje i ograničenje)*

- (1) Podatak se briše ili obrada ograničava kada su ispunjeni zakonski uslovi, osim ako je čuvanje potrebno zbog zakonske obaveze, javnog interesa, arhiviranja, istraživanja ili pravnog zahtjeva.

#### **Član 35.**

*(Prigovor)*

- (1) Kada se obrada zasniva na javnom ili legitimnom interesu, lice može uložiti prigovor iz razloga koji se odnose na njegov položaj, a direktni marketing prestaje po prigovoru bez dodatnog odmjeravanja.

**Član 36.**  
(Prenosivost)

- (1) Kada su ispunjeni zakonski uslovi, lice dobija podatke koje je dalo u strukturisanom, uobičajenom i mašinski čitljivom formatu ili traži njihov prenos drugom kontroloru ako je tehnički moguć.

**Član 37.**  
(Pritužba i sudska zaštita)

- (1) Lice se obavještava o pravu da se obrati Agenciji za zaštitu ličnih podataka u Bosni i Hercegovini i nadležnom sudu, bez uskraćivanja internog rješavanja zahtjeva.

**Član 38.**  
(Evidencija zahtjeva)

- (1) Zahtjev, provjera identiteta, odluka, rok i izvršene radnje evidentiraju se uz zaštitu sadržaja i ograničen rok čuvanja.

**V KLASIFIKACIJA I UPRAVLJANJE PRISTUPOM**

**Član 39.**  
(Klasifikacija informacija)

- (1) Informacije se prema posljedici neovlaštenog otkrivanja, izmjene ili gubitka razvrstavaju najmanje kao javne, interne, povjerljive i strogo povjerljive.
- (2) Vlasnik informacije određuje oznaku i uslove obrade, a viša zaštita primjenjuje se kada postoji sumnja.

**Član 40.**  
(Javne informacije)

- (1) Javna informacija može se objaviti tek nakon provjere tačnosti, ovlaštenja, autorskih prava i zaštite ličnih i povjerljivih podataka.

**Član 41.**  
(Princip najmanjeg pristupa)

- (1) Pristup se dodjeljuje samo u obimu i trajanju potrebnom za ulogu; privilegovani i masovni pristup posebno se odobrava, evidentira i periodično provjerava.

**Član 42.**  
(Korisnički nalozi)

- (1) Svaki korisnik koristi lični nalog; zajednički nalog dopušta se samo kada je tehnički nužan, uz imenovane korisnike i dodatnu sljedivost.

**Član 43.**  
(Lozinke i višefaktorska autentifikacija)

- (1) Lozinke moraju biti jedinstvene i dovoljno jake, ne šalju se nezaštićenim kanalom i ne dijele se drugom licu.
- (2) Višefaktorska autentifikacija primjenjuje se za administrativne, udaljene, cloud i druge naloge povećanog rizika kada je tehnički dostupna.

#### **Član 44.**

*(Promjena i prestanak uloge)*

- (1) Pristup se mijenja odmah po promjeni radne ili studijske uloge i ukida bez odlaganja po prestanku osnova, uz povrat opreme, prenos službenih zapisa i zabranu korištenja tuđeg naloga.

#### **Član 45.**

*(Periodična revizija pristupa)*

- (1) Vlasnik sistema i odgovorno lice periodično provjeravaju aktivne naloge, privilegije, neaktivne korisnike i izuzetke i dokumentuju potrebne promjene.

#### **Član 46.**

*(Evidentiranje pristupa)*

- (1) Kritični sistemi evidentiraju prijave, administrativne radnje, promjene podataka i izvoz u obimu razmjernom riziku; zapis se štiti od izmjene i koristi samo za zakonitu svrhu.

### **VI TEHNIČKE I ORGANIZACIONE MJERE**

#### **Član 47.**

*(Upravljanje rizikom)*

- (1) Visoka škola periodično identifikuje prijetnje, ranjivosti, posljedice i postojeće kontrole, određuje prihvatljiv nivo rizika i plan mjera sa odgovornim licem i rokom.

#### **Član 48.**

*(Fizička sigurnost)*

- (1) Prostori sa dokumentacijom, serverima, mrežnom i drugom kritičnom opremom imaju kontrolisan pristup, zaštitu od požara, vode, prekida napajanja i neovlaštenog ulaska.

#### **Član 49.**

*(Čist sto i čist ekran)*

- (1) Povjerljivi dokumenti ne ostavljaju se bez nadzora, štampa se preuzima odmah, a ekran se zaključava pri svakom napuštanju radnog mjesta.

#### **Član 50.**

*(Službeni uređaji)*

- (1) Službeni uređaj se konfiguriše i održava odobrenim postavkama, šifrovanjem kada je primjereno, zaštitom od zlonamjernog softvera, automatskim zaključavanjem i redovnim ažuriranjem.

#### **Član 51.**

*(Privatni uređaji)*

- (1) Privatni uređaj pristupa službenim podacima samo po odobrenoj politici, uz odvajanje podataka, zaštitu pristupa, mogućnost uklanjanja službenih podataka i zabranu lokalnog čuvanja kada rizik nije prihvatljiv.

## **Član 52.**

*(Rad na daljinu)*

- (1) Pri radu van prostora Visoke škole korisnik štiti ekran i razgovor od drugih lica, koristi odobrenu vezu i kanal, ne ostavlja opremu bez nadzora i izbjegava javne uređaje i nezaštićene mreže.

## **Član 53.**

*(Elektronska pošta i poruke)*

- (1) Službena komunikacija koristi odobrene naloge; prije slanja provjeravaju se primalac, prilog, nivo povjerljivosti i potreba šifrovanja ili sigurnog linka.
- (2) Sumnjiva poruka, link ili zahtjev za lozinku prijavljuje se i ne otvara bez provjere.

## **Član 54.**

*(Prenosni mediji)*

- (1) USB i drugi prenosni medij koristi se samo kada je potreban i odobren, uz provjeru, evidenciju i šifrovanje za povjerljive podatke.

## **Član 55.**

*(Usluge u oblaku)*

- (1) Cloud usluga koristi se nakon pravne, sigurnosne i ugovorne procjene lokacije podataka, podizvođača, pristupa, rezervnih kopija, izvoza i prestanka usluge.

## **Član 56.**

*(Šifrovanje)*

- (1) Povjerljivi i strogo povjerljivi podaci šifruju se u prenosu i, prema procjeni rizika, u mirovanju; ključevi se čuvaju odvojeno i pod kontrolisanim pristupom.

## **Član 57.**

*(Ažuriranja i ranjivosti)*

- (1) Sistemi i aplikacije održavaju se podržanim verzijama, sigurnosna ažuriranja primjenjuju prema kritičnosti, a poznata ranjivost prati do otklanjanja ili prihvatanja preostalog rizika.

## **Član 58.**

*(Zaštita od zlonamjernog softvera)*

- (1) Primjenjuju se tehničke kontrole, filtriranje i obuka protiv zlonamjernog softvera, phishinga i socijalnog inženjeringa, uz ograničenje instaliranja neodobrenog softvera.

## **Član 59.**

*(Razvoj i promjene sistema)*

- (1) Nova aplikacija i značajna promjena prolaze specifikaciju sigurnosnih i privatnosnih zahtjeva, testiranje, odobrenje, plan povratka i razdvajanje razvojnih i produkcijskih podataka.

## **Član 60.**

*(Testni podaci)*

- (1) Stvarni lični podaci ne koriste se u testnom okruženju ako se cilj može ostvariti sintetičkim, anonimizovanim ili odgovarajuće pseudonimizovanim podacima.

#### **Član 61.**

*(Rezervne kopije)*

- (1) Za ključne podatke izrađuju se odvojene i zaštićene rezervne kopije prema utvrđenoj učestalosti i roku, a mogućnost oporavka periodično se testira.

#### **Član 62.**

*(Kontinuitet rada)*

- (1) Plan kontinuiteta određuje kritične usluge, odgovorna lica, alternativne postupke, komunikaciju, prioritet oporavka i prihvatljiv gubitak podataka.

#### **Član 63.**

*(Papirna dokumentacija)*

- (1) Papirni spisi čuvaju se u zaključanom i pristupom kontrolisanom prostoru, iznose samo uz odobrenje i prenose u zatvorenoj ambalaži koja štiti sadržaj.

#### **Član 64.**

*(Uništavanje i brisanje)*

- (1) Dokument i medij po isteku roka uništavaju se tako da se podatak ne može razumno rekonstruisati; brisanje iz sistema i rezervnih kopija provodi se prema dokumentovanom postupku.

### **VII DOSTAVLJANJE, OBJAVLJIVANJE I MEĐUNARODNI PRENOS**

#### **Član 65.**

*(Interno dostavljanje)*

- (1) Podatak se unutar Visoke škole dostavlja samo licu koje ima ovlaštenje i stvarnu potrebu, kroz odobren kanal i u najmanjem potrebnom obimu.

#### **Član 66.**

*(Dostavljanje trećem licu)*

- (1) Prije dostavljanja provjeravaju se identitet primaoca, pravni osnov, svrha, obim, sigurnost kanala i obaveza evidentiranja; usmeni ili neformalni zahtjev ne zamjenjuje potreban pravni osnov.

#### **Član 67.**

*(Javno objavljivanje)*

- (1) Lični podatak se objavljuje samo kada je objava propisana, nužna i razmjerna ili kada postoji valjana saglasnost; prije objave dokument se provjerava radi uklanjanja metapodataka i skrivenih podataka.

#### **Član 68.**

*(Međunarodni prenos)*

- (1) Prenos u drugu državu ili međunarodnu organizaciju provodi se samo kada su ispunjeni zakonski uslovi odgovarajućeg nivoa zaštite, zaštitnih mjera ili dopuštenog izuzetka.
- (2) Cloud lokacija, udaljeni pristup i podrška iz inostranstva smatraju se u procjeni mogućeg prenosa.

### **Član 69.**

*(Rokovi čuvanja)*

- (1) Za svaku kategoriju utvrđuje se rok prema zakonu, svrsi, akreditaciji, zaštiti prava i arhivskim obavezama, nakon čega se podatak briše, anonimizuje ili predaje nadležnom arhivu.

## **VIII INCIDENTI I POVREDA LIČNIH PODATAKA**

### **Član 70.**

*(Obaveza prijave incidenta)*

- (1) Svako lice odmah prijavljuje izgubljen uređaj ili dokument, pogrešno poslan podatak, neovlašten pristup, phishing, zlonamjerni softver, prekid, izmjenu ili drugi sumnjiv događaj kroz objavljeni kanal.
- (2) Prijava u dobroj vjeri ne smije izazvati odmazdu.

### **Član 71.**

*(Početno reagovanje)*

- (1) Odgovorno lice evidentira prijavu, ograničava posljedice, čuva dokaze, sprečava dodatni gubitak i uključuje potrebne stručne, pravne i rukovodne funkcije.

### **Član 72.**

*(Procjena povrede)*

- (1) Procjenjuju se vrsta i obim podataka, broj lica, mogućnost identifikacije, posljedice, ranjivost pogođenih lica, trajanje i djelotvornost preduzetih mjera.

### **Član 73.**

*(Obavješćavanje Agencije)*

- (1) Povreda ličnih podataka prijavljuje se Agenciji bez odlaganja, a kada je moguće najkasnije 72 sata od saznanja, osim ako nije vjerovatno da će predstavljati rizik za prava i slobode lica.
- (2) Ako prijava kasni, navode se razlozi, a informacije se mogu dostavljati fazno kada zakon to dopušta.

### **Član 74.**

*(Obavješćavanje pogođenog lica)*

- (1) Kada je vjerovatan visok rizik, pogođeno lice se obavještava jasnim jezikom o prirodi povrede, kontaktu, mogućim posljedicama, preduzetim mjerama i koracima koje može samo preduzeti, osim kada zakon dopušta izuzetak.

### **Član 75.**

*(Evidencija incidenata)*

- (1) Svaki incident i povreda dokumentuju se sa činjenicama, procjenom, odlukama, obavještenjima, mjerama i naučenim lekcijama, bez obzira da li je prijava Agenciji bila potrebna.

#### **Član 76.**

*(Naknadna analiza)*

- (1) Nakon ozbiljnog incidenta utvrđuju se osnovni uzrok, korektivne i preventivne mjere, rokovi i odgovorna lica, a djelotvornost se naknadno provjerava.

### **IX OBUKA, NADZOR I ZAVRŠNE ODREDBE**

#### **Član 77.**

*(Obuka)*

- (1) Svi korisnici prije pristupa podacima prolaze početnu obuku, a periodično i ciljano usavršavanje obuhvata phishing, lozinke, sigurno dijeljenje, prava lica, incidente i specifične rizike uloge.

#### **Član 78.**

*(Provjera usklađenosti)*

- (1) Službenik za zaštitu podataka, odgovorno lice za sigurnost, interna kontrola ili ovlašteni stručnjak provode periodične i vanredne provjere uz najmanji potreban pristup podacima.

#### **Član 79.**

*(Korektivne mjere)*

- (1) Za nalaz se određuju rizik, mjera, odgovorno lice, rok i dokaz izvršenja; neposredna opasnost ograničava se odmah, čak i ako trajno rješenje zahtijeva duži rok.

#### **Član 80.**

*(Odgovornost)*

- (1) Namjerno ili krajnje nepažljivo kršenje ovog pravilnika razmatra se prema zakonu, ugovoru i opštim aktima, uz razmjernost i pravo lica da se izjasni.
- (2) Nenamjerna greška koja je odmah prijavljena uzima se u obzir kao važna olakšavajuća okolnost.

#### **Član 81.**

*(Godišnji izvještaj)*

- (1) Najmanje jednom godišnje razmatraju se rizici, prava lica, incidenti, obuke, dobavljači, revizije, stanje mjera i plan unapređivanja, uz zaštitu povjerljivih detalja.

#### **Član 82.**

*(Operativna uputstva)*

- (1) Direktor može donijeti tehnička i operativna uputstva za lozinke, pristup, rezervne kopije, mobilne uređaje, incidente i rokove čuvanja, pod uslovom da su usklađena sa ovim pravilnikom i zakonom.

#### **Član 83.**

*(Prestanak važenja)*

- (1) Danom stupanja na snagu ovog pravilnika prestaje da važi Procedura o zaštiti podataka i informacijskoj sigurnosti od 30. marta 2020. godine.

**Član 84.**

*(Stupanje na snagu)*

- (1) Ovaj pravilnik stupa na snagu osmog dana od dana objavljivanja na službenoj oglasnoj ploči i internet stranici Visoke škole.

Broj: \_\_\_\_\_

PREDSJEDNIK SENATA

Brčko, juli 2026. godine

\_\_\_\_\_

