

**BOSNA I HERCEGOVINA
FEDERACIJA BOSNE I HERCEGOVINE
FEDERALNO MINISTARSTVO KULTURE I ŠPORTA
FEDERALNO MINISTARSTVO KULTURE I ŠPORTA**

**PROCEDURE INFORMACIJSKE I KIBERNETIČKE SIGURNOSTI
U FEDERALNOM MINISTARSTVU KULTURE I ŠPORTA**

ožujak, 2026. godine

Na temelju članka 56. Zakona o organizaciji organa uprave u Federaciji Bosne i Hercegovine („Službene novine Federacije BiH“, br. 35/05), federalna ministrica kulture i športa donosi

Procedure informacijske i kibernetičke sigurnosti u Federalnom ministarstvu kulture i športa

Članak 1. (Predmet)

- (1) Ovim Procedurama uređuju se pravila i mjere informacijske i kibernetičke sigurnosti u Federalnom ministarstvu kulture i športa (u daljnjem tekstu: Ministarstvo).
- (2) Procedurama se posebno uređuju:
 - zaštita informacijskih sustava i podataka,
 - pravila korištenja informatičke opreme,
 - upravljanje pristupom sustavima,
 - sigurnost elektroničke komunikacije,
 - postupanje u slučaju sigurnosnih incidenata,
 - održavanje i nadzor informacijskih sustava.

Članak 2. (Svrha)

Svrha ovih Procedura je zaštita informacijskih resursa Ministarstva, sprječavanje neovlaštenog pristupa sustavima i podacima, smanjenje rizika od kibernetičkih napada te osiguranje sigurnog i kontinuiranog rada informacijske infrastrukture.

Članak 3. (Informacijski resursi)

Informacijski resursi Ministarstva obuhvaćaju:

- računalnu i mrežnu opremu,
- informacijske sustave i aplikacije,
- baze podataka,
- službene elektroničke račune (e-mail),
- dokumente i digitalne zapise,
- službenu internetsku stranicu.

Članak 4. (Pristup informacijskim sustavima)

- (1) Pristup informacijskim sustavima Ministarstva dopušten je isključivo ovlaštenim korisnicima.
- (2) Svakom korisniku dodjeljuju se jedinstveni pristupni podaci koje je zabranjeno dijeliti s drugim osobama.
- (3) Pristup se dodjeljuje sukladno radnim zadacima i načelu najmanjih potrebnih ovlasti.

Članak 5. (Lozinke i autentifikacija)

- (1) Lozinke moraju sadržavati najmanje osam znakova te kombinaciju velikih i malih slova, brojeva i posebnih znakova.

- (2) Zabranjeno je zapisivanje lozinki na vidljivim mjestima i njihovo dijeljenje.
- (3) U slučaju sumnje na kompromitaciju lozinka se mora odmah promijeniti.
- (4) Gdje je tehnički moguće, obvezno se koristi višefaktorska autentifikacija (MFA).

Članak 6. **(Korištenje elektroničke pošte)**

- (1) Službena elektronička pošta koristi se isključivo u službene svrhe.
- (2) Zabranjeno je korištenje službenih adresa za privatne registracije i neovlaštene servise.

Članak 7. **(Sigurnost elektroničke komunikacije)**

Korisnici su dužni:

- provjeriti pošiljatelja elektroničke pošte prije otvaranja poruka, poveznica i privitaka,
- ne otvarati sumnjive ili nepoznate sadržaje,
- odmah prijaviti sumnjivu komunikaciju ovlaštenoj IT osobi.

Članak 8. **(Instalacija programskih rješenja)**

- (1) Instalaciju softvera na službenu opremu može izvršiti isključivo ovlaštena IT osoba.
- (2) Zabranjena je instalacija neovlaštenih programa ili aplikacija.

Članak 9. **(Sigurnosni incident)**

Sigurnosnim incidentom smatra se svako neovlašteno ili sumnjivo djelovanje koje može ugroziti sigurnost sustava ili podataka.

Članak 10. **(Postupanje u slučaju incidenta)**

U slučaju sumnje na sigurnosni incident korisnik je dužan:

- odmah prekinuti mrežnu vezu (isključiti mrežni kabel ili Wi-Fi),
- ne isključivati uređaj bez upute,
- odmah obavijestiti ovlaštenu IT osobu,
- zabilježiti aktivnosti koje su prethodile incidentu.

Članak 11. **(Sigurnosne kopije)**

- (1) Ministarstvo osigurava redovito sigurnosno kopiranje podataka.
- (2) Pohrana i zaštita podataka provodi se sukladno važećim propisima.

Članak 12. **(Ovlaštena IT osoba)**

- (1) Poslove tehničkog održavanja informacijskog sustava, osnovne sigurnosne mjere i korisničku podršku obavlja državni službenik raspoređen na radno mjesto viši referent – operater, kao ovlaštena IT osoba u Ministarstvu.
- (2) Ovlaštena IT osoba:
 - provodi osnovne mjere informacijske i kibernetičke sigurnosti,

- pruža tehničku podršku korisnicima,
- sudjeluje u rješavanju sigurnosnih incidenata,
- surađuje s vanjskim izvršiteljem IT usluga.

Članak 13. (Održavanje sustava)

- (1) Tehničko održavanje informacijske opreme, servera i informacijskog sustava Ministarstva obavlja ovlašteni izvršitelj sukladno zaključenom ugovoru o održavanju IT opreme i web stranice.
- (2) Izvršitelj iz stavka (1) ovog članka obavlja poslove održavanja, nadzora sustava, instalacije i ažuriranja programskih rješenja te pruža tehničku podršku korisnicima sustava.
- (3) Izvršitelj je dužan postupati sukladno važećim propisima o zaštiti podataka i sigurnosti informacijskih sustava te u skladu s ugovorom zaključenim s Ministarstvom.

Članak 14. (Službena internetska stranica)

- (1) Ministarstvo koristi službenu internetsku stranicu radi informiranja javnosti o svom radu.
- (2) Informacije objavljene na internetskoj stranici imaju prvenstveno informativni karakter.

Članak 15. (Ograničenje odgovornosti)

- (1) Ministarstvo ne preuzima odgovornost za eventualnu štetu nastalu korištenjem informacija objavljenih na internetskoj stranici.
- (2) Internetska stranica može sadržavati poveznice na druge web stranice za koje Ministarstvo ne odgovara.

Članak 16. (Odgovornost za provedbu)

Za provedbu ovih Procedura odgovorni su:

- djelatnici Ministarstva,
- ovlaštena IT osoba (viši referent – operater),
- vanjski izvršitelj IT usluga.

Članak 17. (Stupanje na snagu)

Ove Procedure stupaju na snagu danom donošenja.

Broj: 06-45-1305/26 DF

Datum: 18. 3. 2026. godine


MINISTRICA

Sanja Vlasisavljević