Advocacy Center
for Democratic Culture

PRAKSE SAJBER BEZBEDNOSTI NA INTERNETU I PROCEDURE DIGITALNE BEZBEDNOSTI

Usvojeno: 2026
Odnosi se na: sve zaposlene, konsultante, volontere i spoljne saradnike

www.acdc-kosovo.org

1. Svrha i obim

Ovaj dokument definiše interne standarde sajber bezbednosti, pravila digitalne bezbednosti i mehanizme zaštite podataka organizacije ACDC. Njegov osnovni cilj je da obezbedi zaštitu osetljivih organizacionih podataka, informacija o donatorima, evidencija korisnika, finansijske dokumentacije i komunikacionih sistema.

Ova politika uspostavlja preventivne mere protiv sajber pretnji kao što su fišing napadi, pokušaji hakovanja, infekcije malverom, socijalni inženjering, krađa identiteta i neovlašćen pristup digitalnim platformama.

Ove procedure se primenjuju na sve kancelarije ACDC-a (Severna Mitrovica, Priština, Beograd), uključujući sve službene uređaje, servere, cloud servise, veb-sajtove, platforme društvenih mreža, interne baze podataka i komunikacione alate koji se koriste u profesionalne svrhe.

2. Identifikovani rizici i organizacioni odgovor

Nakon internih procena i prethodnih sajber incidenata, uključujući proboj na zvanične naloge na društvenim mrežama, ACDC je identifikovao nekoliko strukturnih i operativnih ranjivosti. One su uključivale nestabilno internet rutiranje, nedostatak centralizovanog skladištenja podataka, nedovoljnu primenu višefaktorske autentifikacije i ograničenu strukturisanu svest zaposlenih o sajber bezbednosti.

Kao odgovor na to, ACDC je sproveo sveobuhvatne korektivne mere, uključujući:

- Uvođenje Starlink-a kao zvaničnog internet provajdera kako bi se obezbedila stabilna i bezbedna konekcija.
- Uspostavljanje zvaničnih Meta Business profila sa kontrolisanim administrativnim pristupom.
- Instalaciju centralizovanog internog servera za bezbedno upravljanje dokumentima.
- Implementaciju antivirus softvera na svim službenim uređajima.
- Obavezne obuke zaposlenih o sajber bezbednosti.
- Uvođenje internih protokola za reagovanje na incidente.

Ove mere značajno smanjuju operativne rizike i unapređuju digitalnu otpornost organizacije.

3. Internet i mrežna bezbednost

ACDC koristi Starlink kao svog zvaničnog internet provajdera kako bi obezbedio stabilan, šifrovan i pouzdan pristup internetu. Mrežna infrastruktura je zaštićena lozinkom, a pristupni podaci su dostupni isključivo ovlašćenom tehničkom osoblju.

Organizacija primenjuje sledeće standarde mrežne bezbednosti:

- Snažnu enkripciju lozinki na nivou rutera.
- Periodične promene lozinki.
- Razdvajanje interne mreže i mreže za goste (gde je primenljivo).
- Ograničene dozvole za daljinski pristup.
- Praćenje neuobičajene mrežne aktivnosti.

Neovlašćena instalacija mrežne opreme ili deljenje mrežnih pristupnih podataka strogo je zabranjeno.

4. Centralizovani server i upravljanje podacima

ACDC je implementirao centralizovani interni server kako bi regulisao skladištenje fajlova, smanjio zavisnost od eksternog prenosa dokumenata i obezbedio strukturisano upravljanje dokumentacijom.. Server omogućava:

- Kontrolisan pristup na osnovu radnih uloga zaposlenih.
- Bezbedno skladištenje finansijske, pravne i programske dokumentacije.
- Smanjenu zavisnost od ličnih uređaja prilikom razmene dokumenata.
- Organizovanu strukturu podataka kako bi se sprečilo dupliranje i gubitak podataka.

Redovne rezervne kopije (backup) se prave i čuvaju u zaštićenim okruženjima. Cloud servisi koje koristi ACDC zaštićeni su dvofaktorskom autentifikacijom i procedurama kontrole pristupa. Prava pristupa se odmah ukidaju nakon prestanka radnog odnosa ili saradnje sa konsultantima.

5. Bezbednost uređaja

Svi službeni laptopovi i kancelarijski računari opremljeni su licenciranim antivirus softverom (npr. NOD32 ili ekvivalent). Automatska bezbednosna ažuriranja su uključena kako bi se obezbedila zaštita od novih i nastajućih pretnji.

Standardi korišćenja uređaja uključuju:

- Obaveznu zaštitu lozinkom na svim uređajima.
- Automatsko zaključavanje ekrana nakon perioda neaktivnosti.
- Zabranu instaliranja neovlašćenog softvera.
- Zabranu korišćenja javnih računara za pristup službenim nalozima.
- Bezbedno čuvanje uređaja kada se ne koriste.

USB uređaji i eksterni diskovi moraju biti skenirani pre upotrebe. Izgubljeni ili ukradeni uređaji moraju se odmah prijaviti.

6. Zaštita društvenih mreža i onlajn prisustva

Nakon neovlašćenog pristupa nalozima na društvenim mrežama, ACDC je dodatno ojačao upravljanje svojim digitalnim platformama. Mere uključuju:

- Korišćenje isključivo zvaničnih Meta Business Suite naloga.
- Obaveznu dvofaktorsku autentifikaciju na svim platformama društvenih mreža.
- Administrativni pristup zasnovan na ulogama (primarni: službenik za komunikacije; rezervni: izvršni direktor).
- Hitno uklanjanje pristupa za bivše zaposlene.
- Bezbedno čuvanje lozinki korišćenjem alata za upravljanje lozinkama..

Samo ovlašćeno osoblje ima pravo da objavljuje ili upravlja zvaničnim sadržajem.

7. Bezbednost elektronske pošte i komunikacije

Sva zvanična komunikacija mora se obavljati putem email naloga sa domena @acdc-kosovo.org. Zaposleni su obučeni da prepoznaju phishing poruke, sumnjive priloge i zlonamerne linkove.

Bezbednosne procedure uključuju:

- Zabranu preuzimanja nepoznatih priloga.
- Proveru sumnjivih email poruka sa pošiljaocem putem alternativnog komunikacionog kanala.
- Hitno prijavljivanje potencijalnih phishing pokušaja.
- Redovno ažuriranje lozinki i aktiviranje dvofaktorske autentifikacije (2FA).

Poverljivi podaci o donatorima i korisnicima nikada se ne smeju deliti putem nezaštićenih aplikacija za razmenu poruka.

8. Jačanje kapaciteta zaposlenih i podizanje svesti

Prepoznajući da je ljudska greška jedan od glavnih rizika u oblasti sajber bezbednosti, ACDC organizuje strukturisane obuke kako bi unapredio svest zaposlenih o digitalnim pretnjama.

Teme obuka uključuju:

- Prepoznavanje phishing pokušaja i zlonamernih veb-sajtova.
- Bezbedno pretraživanje interneta i upravljanje lozinkama.
- Sigurno rukovanje osetljivim podacima.
- Digitalnu higijenu i standarde zaštite privatnosti.
- Odgovorno i etičko korišćenje alata veštačke inteligencije.

Uvodna obuka o sajber bezbednosti uključena je u proces uvođenja u posao za nove zaposlene i volontere.

9. Politika lozinki

ACDC primenjuje standarde za jake lozinke:

- Minimum 12 karaktera.
- Kombinacija velikih i malih slova, brojeva i specijalnih znakova.
- Zabranjeno je korišćenje iste lozinke na više platformi.
- Preporučuje se korišćenje menadžera lozinki.
- Lozinke se ne smeju deliti putem email-a ili aplikacija za razmenu poruka.

Periodična promena lozinki je obavezna za administrativne naloge sa visokim nivoom pristupa.

10. Procedura reagovanja na incidente

U slučaju sumnje na sajber bezbednosni incident, potrebno je odmah preduzeti sledeće korake:

1. Isključiti pogođeni uređaj sa interneta.
2. Obavestiti izvršnog direktora i službenika za komunikacije.
3. Promeniti kompromitovane lozinke.
4. Dokumentovati detalje incidenta.
5. Obavestiti relevantne partnere ili donatore ukoliko je potrebno.
6. Po potrebi obnoviti sisteme iz bezbednih rezervnih kopija.

Nakon incidenta sprovodi se analiza kako bi se utvrdili uzroci i sprečilo ponavljanje sličnih situacija.

11. Zaštita podataka i poverljivost

ACDC upravlja osetljivim ličnim, finansijskim i pravnim podacima uz strogo poštovanje principa poverljivosti.

Mere uključuju:

- Ograničen pristup ličnim podacima korisnika.
- Bezbedno skladištenje pravne dokumentacije.
- Obavezu čuvanja poverljivosti za zaposlene i konsultante.
- Kontrolisano deljenje finansijskih informacija.
- Poštovanje važećih principa zaštite podataka

Osetljive informacije ne smeju se čuvati na ličnim uređajima bez prethodnog odobrenja.

12. Praćenje i revizija

Ova politika sajber bezbednosti se revidira na godišnjem nivou i ažurira u skladu sa tehnološkim napretkom i razvojem organizacije. Unapređenje sajber bezbednosti biće integrisano u strateški okvir ACDC-a za period 2026–2030, čime se obezbeđuje dugoročna digitalna otpornost i spremnost na krizne situacije.

13. Usklađenost

Svi zaposleni, konsultanti i volonteri obavezni su da postupaju u skladu sa ovom politikom. Nepoštovanje standarda sajber bezbednosti može dovesti do internih disciplinskih mera. Izvršni direktor i uprava programa nadgledaju sprovođenje i

www.acdc-kosovo.org

office@acdc-kosovo.org

www.facebook.com/Ngoacdc

www.instagram.com/acdc.kosovo

www.x.com/ngo_acdc