BALKANS FORWARD FOUNDATION

POLITIKA DIGITALNE I INFORMACIONE BEZBEDNOSTI

Balkans Forward Foundation

POLITIKA DIGITALNE I INFORMACIONE BEZBEDNOSTI

Sadržaj

1. SVRHA

2. OBUHVAT PRIMENE

3. OPŠTI PRINCIPI

4. PRISTUP I BEZBEDNOST NALOGA

5. UREĐAJI I FIZIČKA BEZBEDNOST

6. ČUVANJE, REZERVNE KOPIJE I UPRAVLJANJE FAJLOVIMA

7. KOMUNIKACIJA I DELJENJE INFORMACIJA

8. KORIŠĆENJE LIČNIH UREĐAJA I NALOGA

9. OSETLJIVE I VISOKORIZIČNE INFORMACIJE

10. SAJBER RIZICI I DOBRA PRAKSA

11. INCIDENTI I PRIJAVLJIVANJE

12. ODGOVORNOST I NADZOR

13. KRŠENJE POLITIKE

14. POVEZANE POLITIKE

15. REVIZIJA POLITIKE

1. Svrha

Svrha ove Politike digitalne i informacione bezbednosti jeste da obezbedi da Balkans Forward Foundation („Fondacija“) štiti svoje digitalne sisteme, uređaje, naloge, komunikaciju, fajlove i osetljive informacije od neovlašćenog pristupa, zloupotrebe, gubitka, oštećenja, otkrivanja ili ometanja rada.

Fondacija prepoznaje da je informaciona bezbednost od suštinskog značaja za integritet organizacije, kontinuitet rada, zaštitu partnera i učesnika, kao i za zaštitu osetljivih informacija povezanih sa ljudskim pravima.

2. Obuhvat primene

Ova politika se primenjuje na sve digitalne sisteme, uređaje, naloge, fajlove, komunikacione alate, platforme i informacije koje Fondacija koristi, kojima pristupa, koje čuva ili kojima upravlja, bilo neposredno ili preko drugih lica.

Primenjuje se na sva lica koja postupaju u ime Fondacije, uključujući osnivača, članove Upravnog odbora, Izvršnog direktora, zaposlene, konsultante, pripravnike, volontere, spoljne eksperte i druga ovlašćena lica.

Ova politika se odnosi i na uređaje u vlasništvu Fondacije i na lične uređaje kada se koriste za potrebe rada Fondacije.

3. Opšti principi

Sva lica koja rukuju informacijama Fondacije ili koriste njene sisteme dužna su da to čine odgovorno, bezbedno i na način koji smanjuje rizik.

Mere zaštite moraju biti srazmerne osetljivosti informacija, nivou rizika i stvarnim operativnim kapacitetima Fondacije.

Informacije moraju biti zaštićene od neovlašćenog pristupa, slučajnog gubitka, krađe, oštećenja ili neprimerenog otkrivanja.

4. Pristup i bezbednost naloga

Pristup sistemima, platformama, fajlovima i nalozima mora biti ograničen isključivo na ovlašćena lica i samo u meri koja je potrebna za obavljanje njihove uloge.

Za naloge i sisteme povezane sa radom Fondacije moraju se koristiti jake i jedinstvene lozinke.

Kada je dostupna, višefaktorska autentifikacija treba da bude uključena za elektronsku poštu, cloud servise, finansijske sisteme, komunikacione alate i druge važne naloge.

Nalozi, lozinke i pristupni podaci ne smeju se deliti, osim kada je to strogo neophodno i na odgovarajući način kontrolisano.

Pristup mora biti uklonjen ili izmenjen bez odlaganja kada dođe do promene uloge ili prestanka angažmana.

5. Uređaji i fizička bezbednost

Laptopovi, telefoni, memorijski uređaji i druga oprema koja se koristi za rad Fondacije moraju se čuvati bezbedno i štititi od krađe, gubitka ili neovlašćenog pristupa.

Uređaji treba da budu zaštićeni lozinkama, PIN kodovima, biometrijskom zaštitom ili drugim odgovarajućim merama pristupa.

Kada je to razumno moguće, uređaji treba da koriste ažuriran softver, operativne sisteme i odgovarajuće bezbednosne zaštite.

Korisnici su dužni da postupaju pažljivo kada rade u javnim prostorima, tokom putovanja ili kada rukuju osetljivim informacijama van bezbednog okruženja.

6. Čuvanje, rezervne kopije i upravljanje fajlovima

Fajlovi i informacije Fondacije treba da se čuvaju na organizovan, bezbedan i primeren način.

Važna dokumentacija ne treba da bude sačuvana isključivo na ličnim uređajima kada to stvara rizik od gubitka ili nedostupnosti.

Kada je to relevantno i izvodljivo, treba koristiti rezervne kopije radi smanjenja rizika od gubitka podataka.

Zajednički folderi, cloud skladišta i alati za saradnju treba da budu organizovani tako da štite poverljivost i spreče nepotrebno izlaganje osetljivih informacija.

7. Komunikacija i deljenje informacija

Komunikacija povezana sa radom Fondacije mora se odvijati na bezbedan i profesionalan način.

Osetljive informacije smeju se deliti samo sa licima kojima su zaista potrebne i putem odgovarajućih kanala.

Poseban oprez mora se primenjivati pri slanju elektronske pošte, deljenju linkova, prosleđivanju dokumenata, korišćenju aplikacija za poruke i komunikaciji o partnerima, korisnicima, učesnicima ili internim pitanjima.

Informacije se ne smeju neformalno deliti niti prenositi putem nesigurnih kanala kada to stvara nepotreban rizik.

8. Korišćenje ličnih uređaja i naloga

Kada se lični uređaji ili nalozi koriste za rad Fondacije, primenjuju se isti standardi pažnje, poverljivosti i bezbednosti.

Fajlovi, kontakti i komunikacija povezani sa Fondacijom treba, kada je to moguće, da budu odvojeni od isključivo privatne upotrebe.

Fondacija može zahtevati da se određene informacije ili pristupi prenesu, obezbede ili uklone po prestanku angažmana.

9. Osetljive i visokorizične informacije

Posebna pažnja mora se posvetiti osetljivim informacijama, uključujući podatke o ličnosti, finansijske podatke, interna organizaciona pitanja, pravnu dokumentaciju, informacije povezane sa zaštitom, kao i sve informacije koje se odnose na osetljiva lica, branioce ljudskih prava, LGBT+ osobe, manjinske zajednice ili partnere koji rade u neprijateljskom ili rizičnom okruženju.

Pristup takvim informacijama mora biti strogo ograničen i zasnovan na principu „samo onoliko koliko je potrebno“.

10. Sajber rizici i dobra praksa

Sva lica koja deluju u ime Fondacije dužna su da budu oprezna u vezi sa phishing pokušajima, sumnjivim elektronskim porukama, lažnim linkovima, nepoznatim prilozima, kompromitovanim nalozima, lažnim predstavljanjem, zlonamernim softverom i drugim digitalnim pretnjama.

Svaka sumnjiva aktivnost ili moguća kompromitacija mora biti odmah prijavljena.

Treba izbegavati preuzimanje nepotrebnog softvera, korišćenje nezaštićenih mreža za osetljiv rad i zaobilaženje razumnih bezbednosnih mera.

11. Incidenti i prijavljivanje

Svaki stvarni ili sumnjivi incident digitalne bezbednosti, uključujući gubitak uređaja, kompromitaciju naloga, neovlašćeni pristup, slučajno otkrivanje podataka, sumnjivu aktivnost ili povredu podataka, mora se odmah prijaviti Izvršnom direktoru ili drugom odgovornom licu.

Fondacija će preduzeti razumne korake radi obuzdavanja, procene i rešavanja bezbednosnih incidenata blagovremeno i srazmerno.

Kada je to relevantno, incidenti se moraju rešavati i u skladu sa Politikom zaštite podataka.

12. Odgovornost i nadzor

Sva lica koja deluju u ime Fondacije odgovorna su za zaštitu informacija i za praktičnu primenu ove politike.

Izvršni direktor odgovoran je za nadzor nad sprovođenjem politike, podizanje svesti o rizicima i obezbeđivanje postojanja razumnih mera zaštite.

Upravni odbor ima nadzornu odgovornost da obezbedi da Fondacija ozbiljno pristupa digitalnoj i informacionoj bezbednosti kao delu dobrog upravljanja.

13. Kršenje politike

Nepridržavanje ove politike može dovesti do korektivnih ili disciplinskih mera, u zavisnosti od ozbiljnosti povrede.

Ozbiljna nepažnja, namerna zloupotreba, prikrivanje incidenata ili neovlašćeno otkrivanje osetljivih informacija mogu se smatrati ozbiljnim kršenjem ove politike.

14. Povezane politike

Ovu politiku treba čitati zajedno sa Politikom zaštite podataka (GDPR), Politikom čuvanja dokumentacije i arhiviranja, Kodeksom ponašanja, Politikom zaštite, Politikom sprečavanja korupcije i prevara i svim relevantnim zakonskim ili donatorskim zahtevima.

15. Revizija politike

Ova politika će se periodično preispitivati i po potrebi ažurirati radi usklađivanja sa praksom organizacije, digitalnim rizicima, pravnim obavezama i standardima dobrog upravljanja.