Politika upravljanja lozinkama — Dr Tijana

POVERLJIVO — dokument firme „Dr Tijana“ je priprema za Politika upravljanja lozinkama. Ne distribuirati van BDB tima i ovlašćenih lica klijenta.

Datum generisanja: 07.11.2026. 23:17

Dokument je pripremljen na osnovu odgovora klijenta u upitniku za ovu uslugu. Pre usvajanja od strane rukovodstva, sadržaj proveriti, dopuniti i urediti.

1. Svrha i obim primene

Ovaj dokument uređuje pravila za kreiranje, čuvanje, promenu i korišćenje lozinki, kao i upotrebu multifaktorske autentikacije (MFA) u [NAZIV FIRME]. Dokument obavezuje sve zaposlene, angažovana lica i spoljne saradnike koji imaju pristup informacionim sistemima [NAZIV FIRME], uključujući sistem za zakazivanje i vođenje medicinske dokumentacije pacijenata (sistem elektronskog kartona) i sve druge sisteme koji se koriste u poslovanju ordinacije. Pravila iz ovog dokumenta primenjuju se na korisničke, administratorske i servisne/sistemske naloge.

2. Pravila i mere

Minimalna dužina lozinke za sve naloge u [NAZIV FIRME] iznosi 8 karaktera.

Zahtevi u pogledu sastava lozinke (obavezna kombinacija velikih i malih slova, brojeva i specijalnih znakova) [KLIJENT DA DOPUNI: definisati tačan sastav lozinke koji se zahteva za sve naloge].

Lozinke se ne menjaju po unapred utvrđenom vremenskom periodu. Promena lozinke je obavezna isključivo u sledećim slučajevima: po sumnji ili saznanju da je lozinka kompromitovana, nakon bezbednosnog incidenta koji je mogao uticati na nalog, i prilikom resetovanja lozinke u skladu sa procedurom iz tačke 4. ovog dokumenta.

Korišćenje menadžera lozinki (password manager) nije obavezno niti propisano ovim dokumentom.

Multifaktorska autentikacija (MFA) nije obavezna ni za jedan sistem u [NAZIV FIRME] na dan usvajanja ovog dokumenta.

Deljenje korisničkih naloga i lozinki između zaposlenih je izričito zabranjeno. Svaki zaposleni koristi isključivo nalog koji mu je lično dodeljen i ne sme ga ustupati drugom licu,

bez obzira na funkciju ili razlog.

Za servisne i sistemske naloge važe posebna pravila. Servisni nalog za sistem elektronskog kartona koristi isključivo spoljni IT saradnik zadužen za održavanje tog sistema. Lozinku za ovaj nalog poznaju samo spoljni IT saradnik i direktor. Lozinka servisnog naloga ne sme se deliti sa drugim zaposlenima niti sa trećim licima van ovog kruga. Promena lozinke servisnog naloga sprovodi se obavezno u slučaju prestanka saradnje sa spoljnim IT saradnikom ili sumnje na kompromitaciju naloga.

3. Odgovornosti

Direktor, kao lice odgovorno za nadzor nad informacionom bezbednošću i za praćenje usklađenosti sa propisima o informacionoj bezbednosti, odgovoran je za usvajanje i ažuriranje ove politike, odobravanje izuzetaka od opštih pravila (uključujući pravila za servisne naloge) i čuvanje lozinke servisnog naloga za sistem elektronskog kartona.

Spoljni IT saradnik odgovoran je za bezbedno korišćenje i čuvanje lozinke servisnog naloga za sistem elektronskog kartona, kao i za obaveštavanje direktora o potrebi promene te lozinke.

Svaki zaposleni odgovoran je za čuvanje poverljivosti svoje lozinke, nekorišćenje tuđih naloga i prijavljivanje sumnje na kompromitaciju svog naloga direktoru.

[KLIJENT DA DOPUNI: nosilac odgovornosti za sprovođenje procedure provere identiteta prilikom resetovanja lozinke, ukoliko se razlikuje od direktora]

4. Procedure

Procedura bezbednog resetovanja lozinke sprovodi se u sledećim koracima:
Zaposleni koji zahteva reset lozinke obraća se [KLIJENT DA DOPUNI: lice ili kanal kome se zahtev upućuje].
Pre izvršenja reseta, sprovodi se provera identiteta lica koje zahtev podnosi, u skladu sa postojećom procedurom provere identiteta [KLIJENT DA DOPUNI: način provere identiteta, npr. lično prisustvo, provera putem službenog e-maila, telefonska provera uz unapred definisana pitanja].
Nakon potvrde identiteta, lozinka se resetuje i dostavlja zaposlenom na bezbedan način, uz obavezu da je zaposleni izmeni prilikom prve prijave.

Procedura u slučaju sumnje na kompromitaciju lozinke ili naloga:
Zaposleni koji posumnja da je njegova lozinka ili lozinka servisnog naloga kompromitovana dužan je da o tome odmah obavesti direktora.
Direktor nalaže trenutnu promenu kompromitovane lozinke.
U slučaju da je ugrožen servisni nalog za sistem elektronskog kartona, direktor i spoljni IT

saradnik zajednički sprovode promenu lozinke tog naloga bez odlaganja.

Procedura prilikom prestanka angažovanja spoljnog IT saradnika ili zaposlenog:
Direktor nalaže promenu lozinki svih naloga kojima je to lice imalo pristup, uključujući servisni nalog za sistem elektronskog kartona ukoliko je relevantno.

Ovaj dokument stupa na snagu danom usvajanja od strane rukovodstva Dr Tijana.

U _____, ____.____._____. godine

M.P.

Ovlašćeno lice:

_____