Politika upravljanja pristupom — Dr Tijana

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

Datum generisanja: 07.11.2026. 23:19

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

Ova politika uređuje način dodeljivanja, revizije i oduzimanja pristupa informacionim sistemima i podacima u [NAZIV FIRME], sa posebnim osvrtom na pristup sistemu elektronskog kartona pacijenata. Dokument obavezuje sve zaposlene, angažovane saradnike i treća lica kojima je, zbog prirode posla, odobren pristup IKT sistemima i podacima [NAZIV FIRME], uključujući osetljive zdravstvene podatke pacijenata. Cilj politike je da obezbedi da pristup sistemima bude dodeljivan, evidentiran, periodično proveravan i blagovremeno oduzet na kontrolisan način.

2. Pravila i mere

Pristup sistemu elektronskog kartona i drugim informacionim sistemima [NAZIV FIRME] dodeljuje se isključivo na osnovu stvarne potrebe izvršavanja radnih zadataka korisnika. Obim pristupa po principu najmanje privilegije bliže se određuje na sledeći način: [KLIJENT DA DOPUNI: kategorije korisnika (npr. lekar, medicinska sestra, administrativno osoblje) i tačan opseg podataka/funkcija sistema elektronskog kartona kojima svaka kategorija sme da pristupi].

Svaki zahtev za dodelu pristupa mora biti evidentiran u pisanoj ili elektronskoj formi, sa naznakom korisnika, sistema/dela sistema kome se pristup dodeljuje i obrazloženjem poslovne potrebe. Evidencija odobrenih pristupa čuva se trajno dok korisnik ima aktivan nalog, i najmanje [KLIJENT DA DOPUNI: rok čuvanja evidencije nakon oduzimanja pristupa].

Pristup se po prestanku radnog odnosa ili angažmana oduzima najkasnije [KLIJENT DA DOPUNI: tačan rok, npr. istog dana ili u roku od 24 časa od prestanka radnog odnosa]. Do određivanja ovog roka, obaveza je da se nalog korisnika kome prestaje radni odnos deaktivira pre njegovog poslednjeg radnog dana ili najkasnije na taj dan.

Administratorski i drugi privilegovani nalozi (nalozi sa pravom izmene podešavanja sistema, dodele pristupa drugim korisnicima ili pristupa celokupnoj bazi elektronskog

kartona) moraju biti odvojeni od redovnih korisničkih naloga iste osobe, zaštićeni višefaktorskom autentifikacijom (MFA) i podložni evidentiranju (logovanju) svih radnji izvršenih putem takvog naloga. Broj privilegovanih naloga u [NAZIV FIRME] ograničava se na [KLIJENT DA DOPUNI: broj i nosioce privilegovanih naloga].

Prava pristupa svih korisnika sistemu elektronskog kartona i drugim poslovnim sistemima podležu formalnoj periodičnoj reviziji, čiju učestalost određuje [KLIJENT DA DOPUNI: učestalost revizije, npr. svakih šest meseci ili jednom godišnje]. Revizijom se proverava da li dodeljeni pristup i dalje odgovara trenutnoj radnoj ulozi korisnika i da li postoje nalozi koje treba ukinuti ili ograničiti.

3. Odgovornosti

Direktor je odgovoran za odobravanje svakog zahteva za dodelu, izmenu ili oduzimanje pristupa sistemu elektronskog kartona i drugim informacionim sistemima [NAZIV FIRME], kao i za pokretanje i sprovođenje periodične revizije dodeljenih prava pristupa.

Direktor je takođe odgovoran za nadzor nad informacionom bezbednošću na nivou organizacije i za praćenje usklađenosti sa propisima o informacionoj bezbednosti, uključujući primenu ove politike.

Svaki zaposleni i angažovani saradnik dužan je da koristi dodeljeni pristup isključivo u okviru svojih radnih zadataka, da ne deli svoje korisničke podatke sa drugim licima i da bez odlaganja prijavi direktoru svaku uočenu nepravilnost u vezi sa pristupom sistemima (npr. pristup kome nije trebalo da bude dodeljen, sumnju na neovlašćeno korišćenje naloga).

[KLIJENT DA DOPUNI: ukoliko se u budućnosti uvede posebna uloga ili lice zaduženo za administraciju sistema elektronskog kartona (IT administrator), ovde definisati njegovu odgovornost za tehničko sprovođenje dodele/oduzimanja pristupa].

4. Procedure

Dodela pristupa: Zaposleni ili njegov neposredni rukovodilac upućuje zahtev za dodelu pristupa direktoru, sa naznakom sistema i obima pristupa koji je potreban za obavljanje posla. Direktor odobrava ili odbija zahtev i evidentira odluku u skladu sa tačkom 2. ove politike. Pristup se aktivira tek nakon pisanog ili elektronski zabeleženog odobrenja direktora.

Revizija pristupa: U rokovima utvrđenim u tački 2. ove politike, direktor sprovodi proveru svih aktivnih naloga u sistemu elektronskog kartona i drugim poslovnim sistemima, upoređujući dodeljena prava sa trenutnim radnim ulogama korisnika. Nalozi čiji obim pristupa više ne odgovara radnoj ulozi korisnika ograničavaju se ili ukidaju odmah po utvrđivanju neusklađenosti.

Oduzimanje pristupa po prestanku angažmana: Neposredno po saznanju o prestanku radnog odnosa ili angažmana zaposlenog, direktor nalaže deaktivaciju svih njegovih naloga u rokovima utvrđenim u tački 2. ove politike. Deaktivacija se evidentira sa datumom i vremenom izvršenja.

Eskalacija bezbednosnih sumnji u vezi sa pristupom: Svaka prijava neovlašćenog ili sumnjivog pristupa sistemu elektronskog kartona dostavlja se direktoru odmah po uočavanju. Direktor sprovodi proveru prijavljenog slučaja i, ukoliko se sumnja potvrdi, nalaže trenutno ograničavanje ili oduzimanje spornog pristupa, uz evidentiranje preduzetih mera.

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

U _____, ____.____._____. godine

M.P.

Ovlašćeno lice:

_____